(2)

COMPUTER-AIDED ACQUISITION AND LOGISTIC SUPPORT TELECOMMUNICATIONS PLAN

Report PL810R1

August 1989

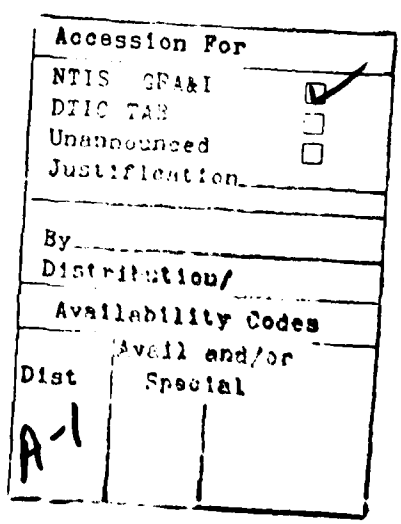
John S. Doby

Prepared pursuant to Department of Defense Contract MDA903-85-C-0139. The views expressed here are those of the Logistics Management Institute at the time of issue but not necessarily those of the Department of Defense. Permission to quote or reproduce any part must – except for Government purposes – be obtained from the Logistics Management Institute.

LOGISTICS MANAGEMENT INSTITUTE
6400 Goldsboro Road
Bethesda, Maryland 20817-5886

ACKNOWLEDGMENTS

The Logistics Management Institute acknowledges the contribution of Frances L. DeLaura, (now at Advanced Technology, Inc.), who wrote the draft of this document. We appreciate the technical advice and written inputs provided by Sandra Heiler and three of her colleagues, Richard Meyer, Chris Reedy, and Susan Radke-Sproull, of the Computer Corporation of America. We also appreciate the technical advice and written inputs provided by Steven Sharp, Joseph Rivera, and Paul Wong of the Federal Data Corporation. The Boeing Company provided significant input to this document. Finally, several Government and industry reviewers provided comments on the draft of the document and we appreciate their thoughtful and helpful review.



Executive Summary

COMPUTER-AIDED ACQUISITION AND LOGISTIC SUPPORT TELECOMMUNICATIONS PLAN

Computer-aided Acquisition and Logistic Support (CALS) is intended to automate technical data and drawing deliverables including technical manuals and computer-aided design/computer-aided manufacturing (CAD/CAM) products. Automated data coupled with a real-time means of access should lower procurement and support costs, increase efficiencies, and result in a greater ability to disseminate and reuse data. To accomplish this, CALS must span multiple functions and databases. Since the functions and databases are not colocated, data transmission requirements and communications protocols are very critical. We recommend a telecommunications architecture and intelligent gateway (IG) architecture for transmitting data over long-haul lines. We recommend making optimal use of the Defense Data Network (DDN) and alternate means for data transmittal should CALS requirements exceed DDN capability.

The telecommunications architecture we recommend specifies that the communications protocols, data exchange protocols, and transmission media to support CALS projects should be implemented in three phases, consistent with the phased Department of Defense migration to Open Systems Interconnection (OSI) standards. The objective is to accommodate CALS distributed computer networks and to enable the interconnection of selected heterogeneous components based on cost, performance, availability, and competitive procurement. This approach is consistent with the overall CALS plan. For full CALS implementation, we recommend three phases:

- Near Term (1989–1990). In the near-term, special attention should be given to the local environment because the bulk of data transfer over geographically dispersed areas will generally be accomplished off line in this timeframe. Usage of DDN should be limited to high-priority/low-bandwidth transmissions.

- Mid Term (1991 – 1992). The ability of the DDN to support all the required protocols should become available during the mid term; however, its use should still be restricted to high-priority/low-bandwidth transmissions.
- Long Term (1993 – 1994). The long-term phase will include the addition of the higher bandwidth physical media required to support on-line transfer of bulk file data associated with CALS projects.

In the period after 1994, growth in CALS applications and traffic will almost certainly involve the use of Integrated Services Digital Network (ISDN) technology and automatic transaction processing. On a local area network (LAN) basis, increased traffic may require multigigabit networks.

We recommend an IG architecture to facilitate retrieval and analysis of data, by logisticians, from distributed applications using dissimilar hardware and software. This access will not require changes to existing databases, database management systems (DBMSs), or application programs. IGs provide transparent log-ons, translate user-prompted queries into a form that can be read by database retrieval programs, and in some cases provide downloading and postprocessing of the retrieved information. An IG may or may not include communications gateway functions along with the application programs written to support user interfaces. Prototype efforts should be initiated in the near term to develop the mid- and long-term IG capabilities.

- Near Term (1989 – 1990). *Basic gateways* are the simplest to implement and can provide benefits for near-term solutions.
- Mid Term (1991 – 1992). *Interoperation gateways* will accept an increased amount of the data access burden, transparent to the user.
- Long Term (1993 – 1994). *Integration gateway systems* focus on semantic issues associated with providing integrated access to information.

This plan is designed to assist in the development of organization-specific communications plans tailored to each CALS effort. Except for proposing optional use of communications facilities, it does not address the integration of CALS telecommunications requirements with those of other DoD efforts such as Electronic Data Interchange (EDI) and Modernization of Defense Logistics Standard Systems (MODELS).

CONTENTS

		Page
Acknowledgments		iii
Executive Summary		v
List of Figures		ix
Section 1.	Introduction	1- 1
1.1	Background	1- 1
1.2	Objectives	1- 1
1.3	Organization of this Plan	1- 2
Section 2.	CALS Telecommunications Architecture	2- 1
2.1	International Standards	2- 3
2.2	ISO Protocol Adoption by DoD	2- 4
2.3	Transmission Volume Requirements	2- 4
2.4	Conformance and Interoperability	2- 5
2.5	CALS Transition Planning	2- 6
Section 3.	Intelligent Gateways	3- 1
3.1	Basic Gateway Systems	3- 2
3.2	Interoperation and Integration Gateway Systems	3- 4
3.3	Expert Front-End Systems	3- 8
3.4	Comparison of Approaches	3- 9
3.5	CALS Intelligent Gateway Development	3-12
Section 4.	Communications Security and Related Issues – A Management Perspective	4- 1
4.1	Background	4- 2
4.2	Legislation and DoD Policy Relevant to CALS	4- 5
4.3	Technical Data Ownership, Responsibilities, and Protection	4- 7
4.4	Developing Security Technologies	4-12

CONTENTS (Continued)

		Page
Glossary		Gloss. 1 – 7
Appendix A.	CALS Data Communications Guideline	A-1 – A-45
Appendix B.	Network Capacity Planning	B-1 – B- 7
Appendix C.	Intelligent Gateways in the CALS Environment	C-1 – C-33
Appendix D.	Commercial and Experimental Intelligent Gateways	D-1 – D-11
Appendix E.	Survey of Relevant Standards Development Efforts	E-1 – E- 7

FIGURES

		Page
2-1.	CALS Communications Architecture	2- 2
2-2.	Near-Term CALS Communications (1989 – 1990)	2- 8
2-3.	Mid-Term CALS Communications (1991 – 1992)	2-11
2-4.	Long-Term CALS Protocols (1993 – 1994) – End Systems	2-14
3-1.	Standards Architecture (Long-Term Target)	3-14
3-2.	Services Architecture (Long-Term Target)	3-15
3-3.	Interoperation Gateway (Intermediate Capability)	3-19
3-4.	Integration Gateway (Target Capability)	3-20

SECTION 1

INTRODUCTION

1.1 BACKGROUND

The Computer-aided Acquisition and Logistic Support (CALS) communications working group is chartered to provide advice and assistance to the CALS steering group in the areas of data transmission requirements and communications protocols. The working group focuses on communications requirements for interfacing with industry and communicating CALS data within DoD.

The first report distributed by the working group, *Assessment of DoD and Industry Networks for Computer Aided Logistics Support (CALS) Telecommunications*,[1] included an evaluation of the telecommunications requirements and the approaches taken by the Services to automate and modernize engineering drawing repositories and technical data repositories; it is also an evaluation of the policy for Service-wide telecommunications planning and implementation, and an evaluation of commercial state-of-the-art communications standards and networks. That report prepared the groundwork for the telecommunications architecture and the intelligent gateway (IG) architecture proposed in this document. This plan recommends guidelines for transmitting data over local area networks (LANs) and long-haul lines, recommends ways to make optimal use of the Defense Data Network (DDN), and contains alternate means for data transmittal should CALS requirements exceed DDN capability. These guidelines are designed to assist in the development of organization-specific communications plans tailored to each CALS effort.

1.2 OBJECTIVES

This CALS telecommunications plan addresses three areas of concern for CALS communications: telecommunications planning in support of CALS programs; IGs to provide user-friendly interfaces with existing and planned operations, as well as a

[1]LMI Report AL636R1. *Assessment of DoD and Industry Networks for Computer Aided Logistics Support (CALS) Telecommunications*. DeLaura, Frances L., Steven J. Sharp, and Richard Clark. Jun 1987.

means for accommodating translation between different graphics and technical data standards; and management issues associated with communications security.

The objectives of the CALS telecommunications plan are to accommodate distributed CALS computer networks and to enable the interconnection of selected heterogeneous components based on cost, performance, availability, and competitive procurement. This plan, or derivatives, can be supplied to vendors as a statement of direction and to industry contractors as the list of standards that will be used to provide interoperability. It is critical that all the parties involved agree on the overall strategy of the plan to ensure successful implementation. To that end, a draft of this plan was widely circulated to industry and Government. Over 521 individuals at 297 organizations had the opportunity to comment on all aspects of the draft plan.

This plan is applicable to all CALS activities and the contractors providing services to them. Specific recommendations are made for meeting local-area and long-haul connectivity requirements for the majority of CALS projects. Organization-specific communications plans must be tailored to the project of interest and take into consideration all the unique factors associated with that project. The plan can assist project managers in the formulation of project-specific communications plans by providing implementation alternatives. This plan does not provide strategies for converting existing implementations to the proposed underlying communications architecture. Except for proposing optimal use of communications facilities, the plan does not address the critical need for integration of CALS telecommunications requirements with those of other DoD efforts, such as Electronic Data Interchange (EDI) and Modernization of Defense Logistics Standard Systems (MODELS).

The plan must be reviewed periodically to incorporate changes in the delivery schedule of proposed standards, vendor product availability, technological advancements, and any future user requirements.

1.3 ORGANIZATION OF THIS PLAN

This section gives a brief introduction to the objectives and content of the plan. In Section 2 we present an overall approach or architecture for CALS telecommunications and a timetable for implementing certain communications functions and protocols. The architecture, presented in full in Appendix A, provides a comprehensive list of data communications protocols, data exchange protocols, and

transmission media to facilitate local and long-haul communications within DoD and between DoD and industry. (Appendix B describes a method for planning network capacity.)

The telecommunications architecture is divided into three phases. Implementation for the near term (1989 – 1990) concentrates on commercially available, off-the-shelf technology; for the mid term (1991 – 1992) on technology that is expected to become stabilized/standardized in that time frame; and for the long term (1993 – 1994) on completing the communications architecture required to support the CALS environment and its specific needs.

In Section 3, we discuss various commercially available and experimental IG products in two categories: basic gateway systems, and interoperation and integration gateway systems. The concept of an expert front-end approach to the user interface for an IG is also discussed. An IG architecture is described in Appendix C by expanding on the issues associated with integration technology as it pertains to the CALS environment. The overall strategy and planning considerations for identifying requirements for the capabilities offered by this technology are also summarized in Appendix C, while selected IGs are described in Appendix D. The architecture concentrates on Layers 6 and 7 of the International Standards Organization (ISO)'s Open Systems Interconnection (OSI) Model, addressing the distinction between simple interfacing and integration/understanding. The following issues are associated with achieving the integration goal:

- Integrating across different data models
- Integrating across different software systems
- Integrating across different business environments
- Providing an effective user interface
- Ensuring data quality
- Addressing performance and security.

Both communications and IGs provide an interim measure for given situations. In the CALS environment, with its mix of Service and industry hardware and software, we are unlikely ever to reach a level of standardization that would warrant

discontinued use of gateways in all situations. (Relevant standards development efforts are shown in Appendix E.)

Section 4 addresses the legal and policy issues associated with communications security. Communications security cannot be adequately addressed without identifying, from a management perspective, the policy and guidelines that must be put in place to ensure the appropriate technology is used effectively and the proper procedures are implemented and followed by everyone in the organization. Legal constraints on the use of software and technical data should be understood by system developers, implementors, and users. Limitations of existing technology and the types of promising network security technology being considered for use in the CALS environment are addressed. The security issues covered include those peculiar to DoD/OSI network interoperation and those created by heterogeneous transmission paths and databases as well as the need for multilayer security.

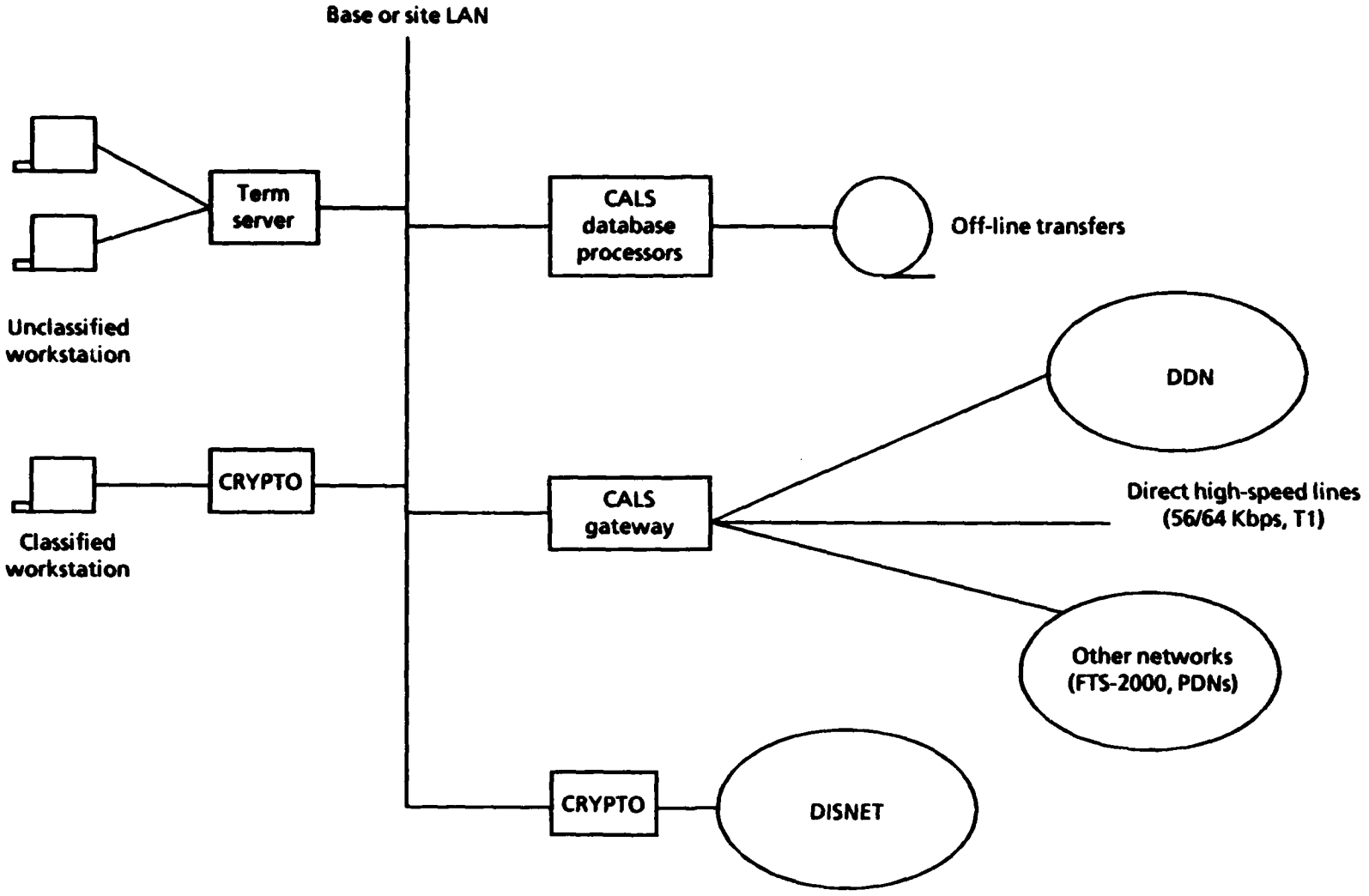
SECTION 2

CALS TELECOMMUNICATIONS ARCHITECTURE

The CALS telecommunications architecture and data communications guideline provides a comprehensive list of data communications protocols, data exchange protocols, and transmission media to be used to facilitate communications among the Military Services, the Defense Logistics Agency (DLA), and industry contractors. The guideline is presented in full in Appendix A; this section describes its most important elements.

The data communications guideline is divided into three chronological phases that serve as a timetable for implementing certain functions and protocols based on the anticipated availability of the required technologies. The protocols and capabilities outlined in each phase are to be implemented by the end of the specified time frame. The near-term communications phase, covering 1989 – 1990, concentrates on commercially available off-the-shelf technology or software that can realistically be developed and implemented in that time frame. During the near-term phase, the DDN is expected to be available for limited use. The mid-term communications phase concentrates on technology that will become stabilized/standardized in the 1991 – 1992 time frame. During that time, the DDN is expected to support all the required protocols. The long-term communications phase, from 1993 to 1994, completes the CALS communications architecture. It should begin to provide the higher bandwidth services required to accommodate the on-line transmission of increased volumes of CALS data. The description of each phase builds upon the capabilities of the preceding phase and contains recommendations for technology refreshment. Recommendations for the transition to the next phase are provided at the end of the near-term and mid-term descriptions.

The generalized CALS network concept is shown in Figure 2-1. In most cases, CALS operations begin at a workstation, proceed through a base or site LAN, move into an intersite gateway, and continue on to the main telecommunications media. Another level of complication is introduced through operation of classified and unclassified networks on DDN.



Note: DISNET = Distribution Network; FTS = Federal Telecommunications System; Kbps = Kilobits per second; PDN = Public Data Network; T1 = 1.544 Megabits per second.

FIG. 2-1. CALS COMMUNICATIONS ARCHITECTURE

2.1 INTERNATIONAL STANDARDS

The adoption of the ISO OSI protocol suite will provide the high degree of interoperability required by the various CALS projects. The standards are developed in stages and evolve as follows:

- Informal draft proposals are circulated in committee and a working draft is developed. During this stage, the majority of content is still open for change.
- The working draft is accepted by the committee and goes out for ballot to the member countries as a draft proposal. During this stage, the content is still subject to change.
- If approved, the draft proposal is updated using the comments on the ballots. It then goes out for a second ballot for progression as a draft international standard. Upon reaching this stage, the content is considered stable enough for a vendor to begin implementation.
- If successful on the second ballot, comments are again incorporated and a final ballot is made for final progression as an international standard. Once the standard reaches this stage, it is considered very stable with few or no further changes made.
- International standards are changed by addenda. The addenda approval cycle is similar to that for an international standard, progressing from proposed draft addendum, to draft addendum, to addendum.

Vendors should generally wait for a standard to reach the draft international standard stage before beginning to develop products based on that standard. The phased migration approach for protocol implementation in the CALS architecture takes into consideration the current status of each protocol as an international standard. Adoption of the international standards by the CALS projects is consistent with the general trends within industry [Technical Office Protocol (TOP) and Manufacturing Automation Protocol (MAP)] and with many of the Services' central telecommunications plans. Compatibility with industry-adopted standards will aid in achieving interoperability between vendors and the Services. Implementing the international suite in new projects will help avoid expensive and disruptive conversions later.

2.2 ISO PROTOCOL ADOPTION BY DoD

The Defense Communications Agency (DCA) is developing a plan for the transition from the currently used DoD suite of protocols to the international protocol suite. Major milestones in that transition are as follows:

- *April 1987: experimental coexistence of the ISO standards with the DoD standards.* OSI protocols could be specified as alternatives or additions to DoD protocols in DoD networks. They were designated experimental due to limited experience and availability. Additionally, full Government Open Systems Interconnection Profile (GOSIP) compliance was not possible due to the lack of a Phase 2 File Transfer Access and Management (FTAM) implementation. This experimental interoperability required the use of prototype dual-protocol gateways because no commercial products were available. Since neither end-system-to-intermediate-system (ES-to-IS) nor intermediate-system-to-intermediate-system (IS-to-IS) routing protocols were available during this period, static tables had to be used for routing.

- *August 1988: full coexistence of equivalent ISO and DoD protocols.* At this point, both protocol suites are functionally equivalent and supported with the inclusion of the two protocols missing in the initial GOSIP baseline [ES-to-IS and the Virtual Terminal Protocol (VTP)]. Additionally, FTAM based on the National Institute of Standards and Technology (NIST) Phase 2 Implementation Agreements will be available in early 1990 allowing full support for GOSIP. IS-to-IS routing in GOSIP will still have to be accomplished through static routing.

- *August 1990: mandatory inclusion of ISO protocols.* ISO protocols will become mandatory for all new acquisitions.

- *April 1995: deletion of DoD protocols as DoD standards.* DCA will discontinue its support for the current DoD protocols 5 years after the mandatory inclusion of ISO protocols.

2.3 TRANSMISSION VOLUME REQUIREMENTS

CALS project managers should carefully evaluate any requirements for transmitting data over a geographically dispersed area because providing on-line, real-time data transfer capabilities can be extremely expensive. The project managers should analyze specific communications requirements and develop formal specifications in order to understand and document those requirements. A cost/benefit analysis should be undertaken to determine whether true requirements exist for on-line, real-time delivery of information.

Two of the crucial elements in defining network requirements are the workload analysis and the development of traffic models. Traffic models should be prepared from estimates of the traffic that will be generated or from statistical sampling of existing hard-copy traffic. Workload models must take into account network overhead within the local-area and long-haul environments and the effect certain protocols and link management techniques may have on system performance. Appendix B is provided to help in determining the types and number of transmission circuits required to support long-haul transmission requirements, as well as transmission requirements of the local environment.

2.4 CONFORMANCE AND INTEROPERABILITY

A major requirement of OSI protocol implementations is adherence to the standards that allow internetworking of protocols implemented on different systems. All the protocols specified in this plan are to be implemented according to the GOSIP baseline or the GOSIP-based specification. The GOSIP specification is based on the NIST OSI workshop agreements. To ensure different implementations of this protocol suite can operate together, two types of testing are required: conformance testing and interoperability testing. The lower layer protocols should be tested for correct operation in end systems and intermediate systems.

Conformance testing addresses protocol implementation at each layer. The code for the protocol is tested in isolation for conformance with the standard. Several organizations are in the process of developing conformance tests and testing services. NIST will certify test systems and conformance test procedures when completed. The CALS project office will be responsible for identifying the requirements and specifying the corresponding user profiles of the CALS specification.

NIST has published protocol test plans for many of the ISO standards. The following three test plans and additional information pertaining to the conformance issue can be obtained from the National Institute of Standards and Technology, Systems and Network Architecture Division, B-217/Technology Building, Gaithersburg, Maryland, 20899. The three test plans are prepared by the Institute for Computer Sciences and Technology (ICST)/Systems and Network Architecture Division (SNA):

- *A Test Plan for the Implementations of ISO Connectionless Network Protocol*, ICST/SNA-85-5

- *A Users Manual for the Connectionless Internet Protocol Test System*, ICST/SNA-85-6
- *A Test Plan for Implementations of the ISO Class 4 Transport Protocol*, ICST/SNA-85-2.

Interoperability testing consists of communicating with implementations of the same protocol suite on heterogeneous systems. The user or an independent third party should conduct this type of testing; the Corporation for Open Systems (COS) is an example of a third-party test conductor. Several organizations are establishing testing services, but thus far no service has been officially recognized. One such service that could provide interoperability testing is the NIST Open Systems Interconnection Network (OSINET). Technical agreements reached and information vital to OSINET participation are documented by NIST.[1]

Conformance and interoperability testing are to be completed before initial protocol implementation and before moving to a future protocol implementation that may incorporate enhancements to a previously implemented protocol and/or the addition of functionality.

2.5 CALS TRANSITION PLANNING

2.5.1 Near-Term Communications (1989 – 1990)

The main emphasis in near-term communications planning is placed on determining what commercially available technology and products we can realistically expect to be available (i.e., developed and implemented) to support CALS projects in the time period. The near-term plan concentrates on areas where we can achieve the highest productivity gains. The protocols recommended are expected to be fully available from most vendors by the end of this phase. By including them as stated requirements, we expect them to become more widely implemented and available from vendors who wish to do business with DoD. Initially, CALS project managers should use temporary vendor solutions until the required protocol support is available; by the end of the near term, however, vendors should be required to comply with and implement the specified protocols.

---

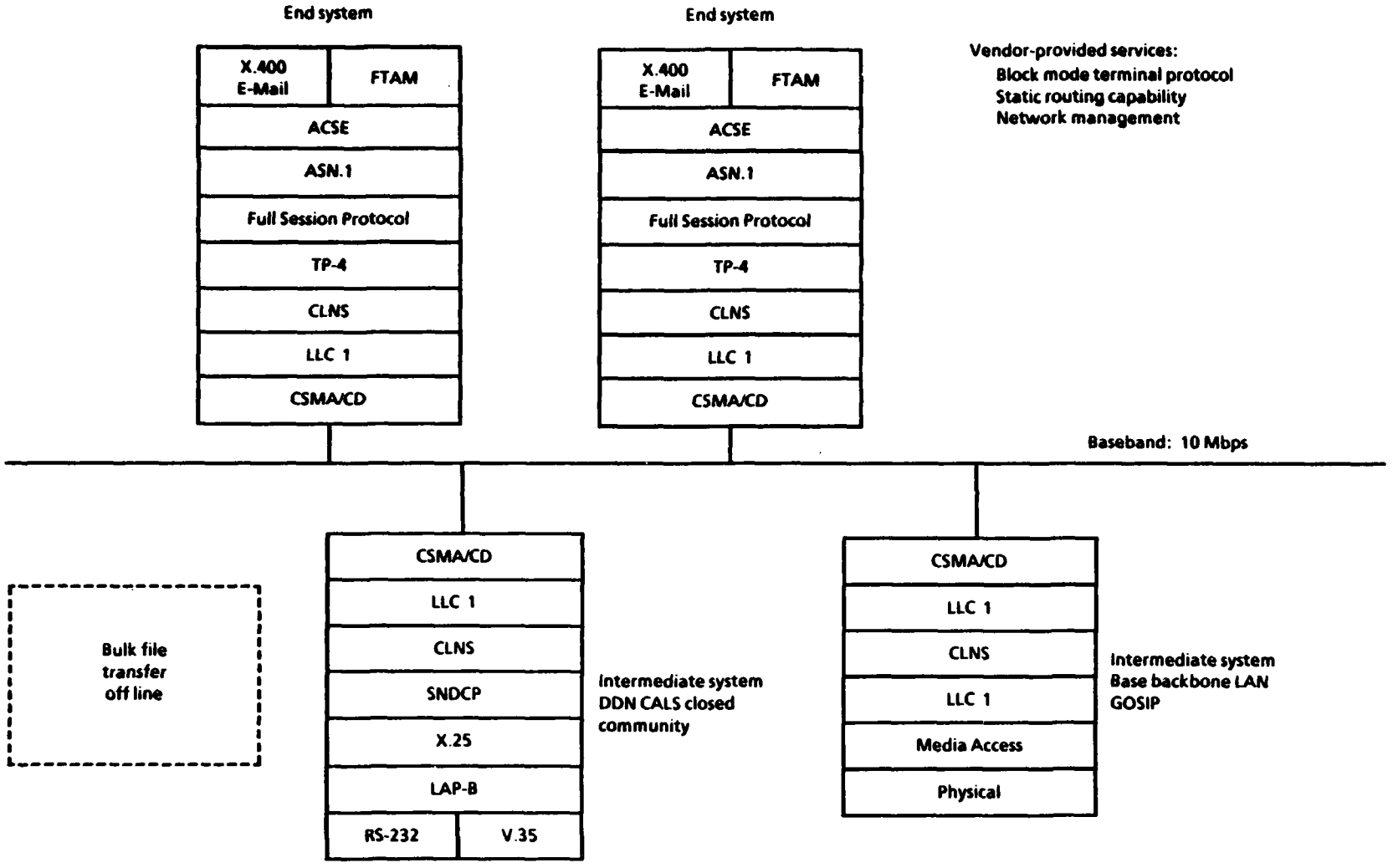
[1] *Implementation Agreements Among Participants of OSINET*. National Bureau of Standards Report NSSIR 86-3478. 1987.

In this phase, we give special attention to the local environment because most of the data transferred over geographically dispersed areas will generally be sent off line. Off-line media such as optical disk, magnetic media, hard copy, etc., will be the most cost-effective method for distributing large volumes of CALS data, and overnight mail will be used for distribution. Standard data exchange protocols and procedures should be followed when using off-line methods of communication.

Figure 2-2 summarizes the near-term communications capabilities. It depicts an ideal local environment in which the protocols implemented in the base or campus LAN are based on the OSI protocols and the GOSIP baseline, eliminating the need for a full gateway system. Connectivity to DDN is provided, but usage is limited to high-priority/low-bandwidth transmissions. Bulk files will be transferred to and from industry and other Government users in an off-line mode. The RS-232 [Electronic Industries Association (EIA) standard interface between data terminating equipment (DTE) and data communications equipment employing serial binary data interchange] is used for low volume requirements at data rates up to 9.6 Kilobits per second (Kbps). Larger data volumes will operate at 56 Kbps using V.35 standards [Consultative Committee on International Telephony and Telegraphy (CCITT) standard governing data transmission at 48 – 64 Kbps].

Each CALS project manager should determine the ability of the existing base LAN to support its transmission requirements, and each CALS project must specify any local requirements for internetworking the CALS LAN to other base or campus type LANs. Project managers should evaluate existing or planned basewide interconnection plans and specify additional interconnection/internetworking hardware and software as required. The exact configuration to use depends on the types of LANs to be internetworked. As often as possible, the baseband (10Base5) standard with Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) should be specified for CALS projects because of its suitability to CALS traffic, widespread availability, and low cost.

Internetworking in the long-haul environment is based on the use of DDN as mandated by DoD. DCA is developing a plan to support coexistence of the ISO protocols and the DDN protocol suite. Use of DDN will be limited until the ES-to-IS, IS-to-IS, and VTP are added to the GOSIP baseline. The absence of VTP will prevent use of the DDN Mini-TAC (Terminal Access Controller) in the near term. A further limitation is imposed by the 56 Kilobits per second (Kbps) transmission rate on



Note: ACSE = Associative Control Service Elements; ASN.1 = Abstract Syntax Notation; CLNS = Connectionless Network Service; LAP-B = Link Access Procedure Balanced; LLC 1 = Logical Link Control Class 1; Mbps = Megabits per second; SNDCP = Subnetwork Dependent Convergence Protocol; TP-4 = Transport Protocol Class 4.

FIG. 2-2. NEAR-TERM CALS COMMUNICATIONS (1989 – 1990)

subscriber access links and backbone media. Until those protocols are included and the physical bandwidth increased, DDN should only be used for inquiry type traffic, electronic mail applications, and high-priority/low-bandwidth file transfer traffic.

Furthermore, until the required dynamic routing protocols are incorporated into the architecture, vendors must provide the mechanisms for static routing and the appropriate service interfaces to modify routing parameters and tables. Vendors must also contractually agree to migrate to the specified standards upon their acceptance by NIST.

If a CALS project requires interoperability with other activities that have DDN protocol implementations [Transmission Control Protocol/Internet Protocol (TCP/IP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), etc.], the project should use the appropriate DDN/OSI protocol gateway. A CALS project that requires interoperability with activities that have implemented communications over DDN, based on a proprietary set of vendor upper-layer protocols, should obtain the appropriate gateway intermediate system. This approach might be particularly applicable in cases where projects integrate CALS data with EDI or MODELS type inquiries and/or transactions.

Network security in a LAN will be restricted to the Data Link Layer (Layer 2). DDN security, in the near term, will consist mainly of KG-84As. The KG-84A is an end-to-end encryption device situated between a host and a C/30 packet-switching node (PSN) or Interface Message Processor (IMP). These devices are generally used on all backbone trunks and on all access lines to classified DDN subscribers. KG-84A devices should be used on those CALS projects that must process classified data. Unclassified users may also use this security mechanism to provide security level separation through the use of different keys for each level.

2.5.2 Mid-Term Communications (1991 – 1992)

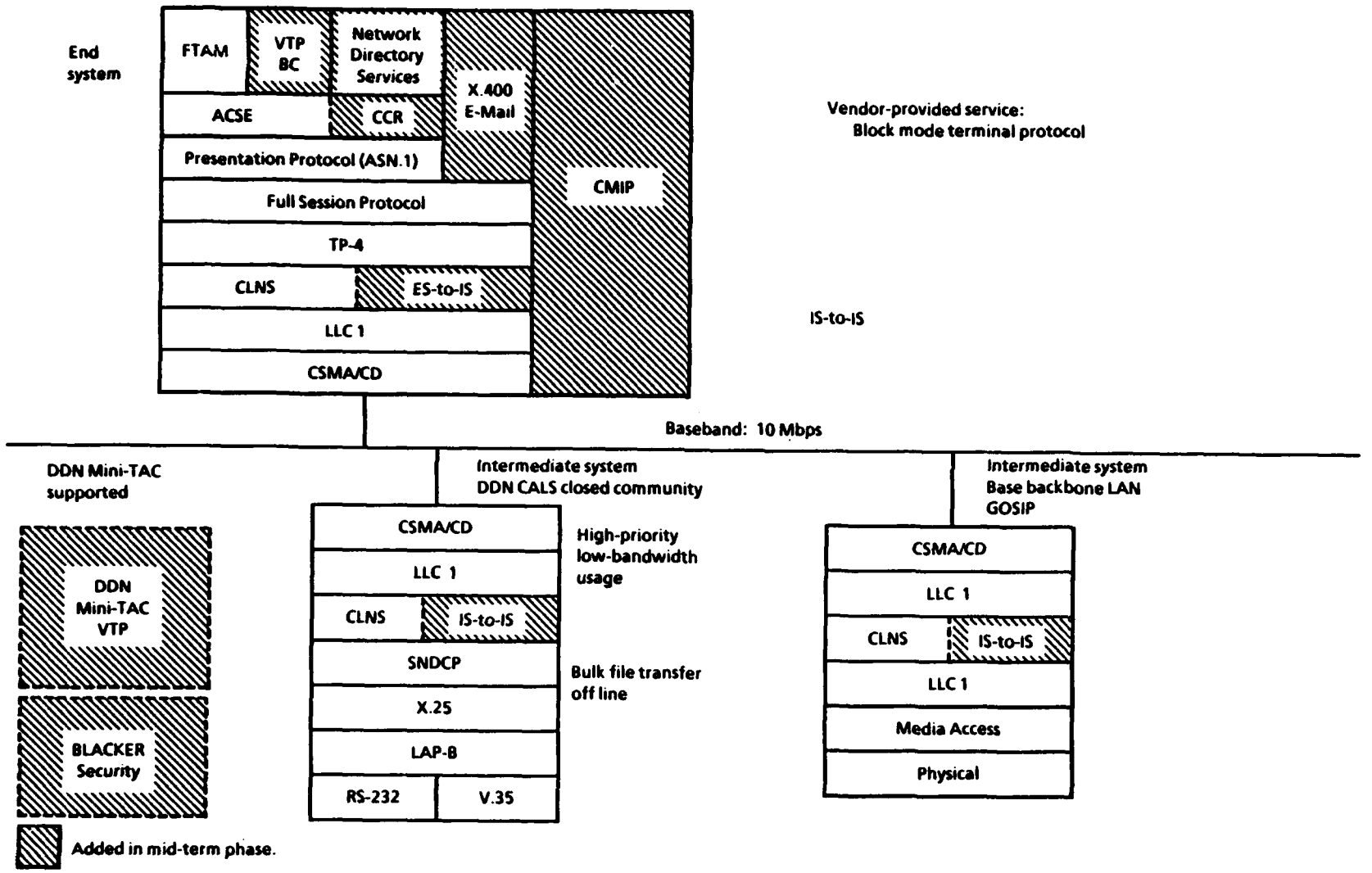
The functionality to be provided by CALS projects in the mid term depends upon the addition of several new protocols, as well as enhancements and additions to protocols specified in the near term. A dynamic internetworking capability is to be added during this time frame. The mid-term phase adds the capability to dynamically route between end systems, whose protocols were defined in the near

term, and the intermediate system that supports interconnection to the DDN or a base/campus LAN.

Figure 2-3 depicts the CALS mid-term communications architecture. The major addition to the CALS architecture is the dynamic routing and network management protocols and VTP. At this time, DCA should introduce the Mini-TAC that incorporates the VTP to support inquiry and mail type applications for remote CALS users. Since the DDN will not have transitioned to a T-series based network, it is likely to still be restricted to high-priority/low-bandwidth transmissions. However, DDN vendors have presented plans that would provide supplemental DDN capability and resources to meet expanded CALS requirements. This plan would graft T1 [1.544 Megabits per second (Mbps)] transmission resources onto the existing DDN environment, and those resources could be allocated and tailored to a specific subscriber community, such as CALS. This system would employ direct point-to-point circuits at T1 or 56 Kbps, or DDN attachments at 56 Kbps. Dial-in X.25 access should be available to small users. This approach offers considerable potential for early CALS applications that require large bandwidths. However, the CALS community will have to approach DDN with specific requirements before DDN can begin expanding its capabilities.

Another capacity option for CALS in the mid term will be the use of the currently contracted Federal Telecommunications System (FTS)-2000 network. FTS-2000 is a state-of-the-art network being developed to augment the Federal Telecommunications System. DoD has not decided the timing and scope for participation in FTS-2000, but it remains a viable option for use with CALS. FTS-2000 could rapidly provide early and economical introduction of Integrated Services Digital Network (ISDN) services to DoD through facilities comparable to emerging public networks. FTS-2000 will feature a full range of voice, data, and video transmission services, which will ultimately be enveloped together in a single integrated switched digital network. Largely based on ISDN technology, FTS-2000 will offer the following services:

- Switched voice
- Switched data
- Switched digital-integrated
- Dedicated transmission.



Note: ACSE = Associative Control Service Elements; ASN.1 = Abstract Syntax Notation; CCR = commitment, concurrence, and recovery; CLNS = Connectionless Network Service; CMIP = Common Management Information Protocol; LAP-B = Link Access Procedure Balanced; LLC 1 = Logical Link Control Class 1; Mbps = Megabits per second; SNDCP = Subnetwork Dependent Convergence Protocol; TP-4 = Transport Protocol Class 4; VTP BC = Virtual Terminal Protocol Basic Class.

FIG. 2-3. MID-TERM CALS COMMUNICATIONS (1991 – 1992)

Even though it can be readily implemented and will provide a large bandwidth, FTS-2000 is a less preferable means of meeting CALS network requirements than DDN expansion because it is incompatible with existing wide-area network (WAN) and LAN facilities. Expansion of DDN would also provide an existing secure network in full compliance with DoD protocols. On the other hand, the DDN approach is likely to result in difficulties in migrating to OSI and in using the technological potential offered by ISDN.

During the mid term, DCA is expected to put a usage charge-back tariff into place. The kilopacket charge will be based on packets of any size, so the maximum packet size of 1.024 million octets, or bytes, should be used. That number may be adjusted depending on throughput and retransmission. We recommend the use of DDN for transmitting nontime-critical data during off-peak times because of the substantial reduction in cost. DDN tariffs must be competitive with those of commercial packet networks.

The BLACKER encryption methodology was first used in January 1989 and is expected to be fully operational during the mid-term period. As is the KG-84A, BLACKER is dependent upon DoD/IP. Unless BLACKER's design specifications are augmented to accommodate ISO/IP's differing header, end-to-end encryption will only be possible for those hosts still employing the old DoD protocol suite. Because DCA has mandated this period for full coexistence of DoD and ISO architectures, we expect BLACKER to be retrofitted to support both DoD/IP and ISO/IP prior to release. Our understanding is that this issue is not yet under study.

During this period, we also expect the first implementations of the Secure Data Network System (SDNS) protocols. The SDNS project was initiated in 1986 by the National Security Agency (NSA) along with NIST, DCA, and several major corporations. Its purpose was to design OSI-conforming protocols to allow implementation of secure computer communications networks. The primary functions of the protocol and resultant secure OSI network architecture are to provide confidentiality, data integrity, authentication, and access control. Current research has resulted in the development of an end-to-end encryption protocol at Layers 3 and 4 of the OSI reference model. If research leads to final products in this time frame, the SDNS approach will lead to more flexible and secure solutions for OSI implementation.

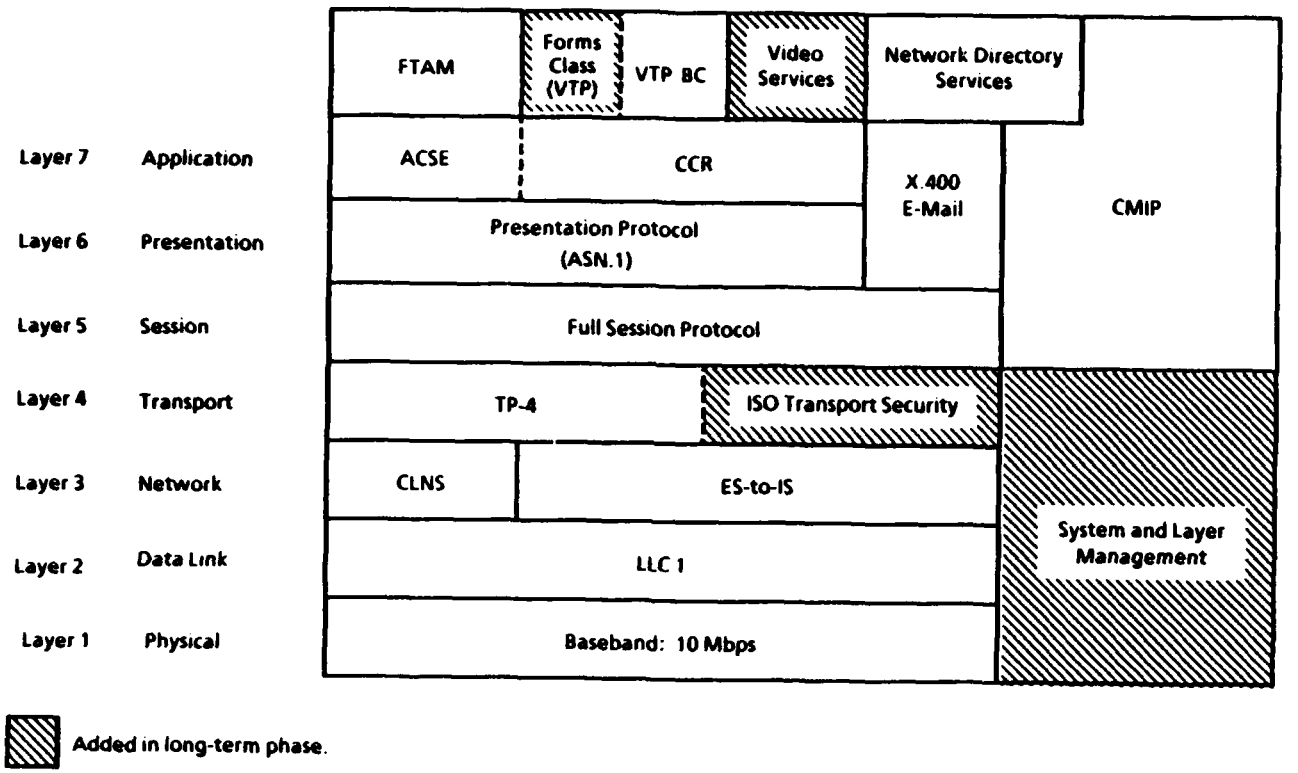
2.5.3 Long-Term Communications (1993 – 1994)

The long-term enhancements to the previously implemented CALS communications architecture involve the implementation of several application layer protocols and the transition to a higher bandwidth media at the Physical Layer, as depicted in Figure 2-4. The CALS project manager should track efforts to standardize the additional protocols and keep abreast of the status of the specified transmission media. Other protocol standards not listed in the guideline may become important to CALS projects in the future and should be added if necessary.

The long-term phase will include the addition of the physical media required to support on-line transfer of bulk file data associated with CALS projects. CALS projects whose volumes dictate the increase in bandwidth should consider migrating to the T1 service if available. If the DDN has not been upgraded to T1 service by this time, the ISDN should be examined as an alternative.

Although the BLACKER encryption methodology holds much promise for use with CALS telecommunications architecture, some concerns exist. BLACKER's ambition for A1 certification and its ability to operate with multisecurity levels, albeit within certain restrictions, makes it an attractive long-term security methodology. BLACKER has been in development for several years; it is expected to be implemented after 1989. Despite its availability in a suitable time frame, BLACKER may be too complex to accommodate changes easily, giving rise to a question of policy: given that DoD is dedicated to an eventual full OSI adoption, what will be the impact when ISO proclaims a network security standard that does not easily accommodate BLACKER?

CALS activities should be guided by the eventual ISO network security standard if it meets DoD requirements. We believe BLACKER can probably be retrofitted to be compatible with the ISO standard. However, since BLACKER is primarily being designed for the classified non-CALS community, we continue to have reservations regarding the utility of its final implementation. Thus, the optimal solution for the CALS network may be the adoption of an approved SDNS protocol. The CALS community may have to press for its release and adoption.



Note: ACSE = Associative Control Service Elements, ASN.1 = Abstract Syntax Notation; CLNS = Connectionless Network Service; CMIP = Common Management Information Protocol; LLC 1 = Logical Link Control Class 1, Mbps = Megabits per second; TP-4 = Transport Protocol Class 4; VTP BC = Virtual Terminal Protocol Basic Class.

FIG. 2-4. LONG-TERM CALS PROTOCOLS (1993 – 1994) – END SYSTEMS

2.5.4 Transaction Processing

In the 1994-plus time frame, more efficient use of CALS resources might be possible through automated transaction processing in which multiple CALS services would be linked through a single request or transaction. If a factory engineer modifies an equipment design, for example, changes in operation and maintenance (O&M) manuals, spare parts inventories, and contracting documentation might occur automatically.

In the current development of specialized services for ISDN, a plan has been developed for incoming call management. In commercial applications, when a customer calls a customer service desk, the call will be accompanied by a calling line identification (CLID), which will automatically be routed to the host mainframe; the mainframe will then respond by forwarding the pertinent customer information to the customer service terminal. Multiple host applications could then be triggered either simultaneously or serially.

Such a mechanism might be adapted for use in CALS automated transaction processing. An incoming CALS transaction of a specific type or origin, for example, might use the same CLID activity to trigger a predetermined series of host applications. The ability to define these applications and their sequences could be provided by the IG, local host, or even by the specific terminal processing the transaction. The selection would be based on a combination of ease of implementation, ease of change, flexibility, and transaction control.

Identification of specific CALS areas that might benefit from transaction processing is outside the scope of this report. However, as the CALS program matures, those areas must be determined. As ISDN implementations are developed for incoming call management, they should be studied for their potential adaptation to the CALS program, particularly if CALS is using or undergoing a transition to ISDN. The CALS program office may also wish to develop and submit a specific ISDN application tailored to CALS use. Of course, transaction processing would not be limited to use on ISDN. Such processing can be developed on any type of CALS network. However, considerable flexibility is inherent in the ISDN design and that flexibility would facilitate such an effort; furthermore, the ISDN program plans to provide services that are closely related to CALS.

The CALS data communications guideline is presented in full in Appendix A. In addition to the architecture described in this section, those guidelines give specific recommendations for meeting security requirements in both local-area and long-haul environments, and architectures for intermediate systems to support communications between heterogeneous systems within each of the time frames.

Appendix B provides a guideline for predicting the amount of network resources required to exchange estimated data.

SECTION 3

INTELLIGENT GATEWAYS

In Section 2, we presented an outline of the basic telecommunications facilities needed for the physical transfer of data in a heterogeneous computer environment. However, effective communication is more than the mere transfer of electronic data; it involves providing access to and transfer of information needed by an *end user*, where the location and format of the information are transparent to the end user.

A goal of CALS is to provide users in the logistics community, easily and effectively from a single device, access to various acquisition and logistics functions resident on heterogeneous computer equipment supported by heterogeneous operating systems. Those devices may be located on a LAN, on LANs accessible through the DDN, or on other communications facilities such as the Automatic Digital Network (AUTODIN), commercial networks, or dedicated communications lines.

Logisticians need to be able to use a single query language and database schema to efficiently access data in preexisting, heterogeneous, distributed applications without making changes to preexisting databases, their database management systems (DBMSs), or their application programs. An IG is a system that facilitates retrieval and analysis of data from systems using dissimilar hardware and software. An IG may include communications gateway functions along with the higher level application programs written to support the required user interfaces. IGs handle transparent log-ons, translate user-prompted queries into a form that can be read by database retrieval programs, and in some cases, provide downloading and postprocessing of the retrieved information. Their most successful use to date has been in commercially supported bibliographic retrieval systems. IGs have also been used successfully for accessing engineering databases.

All IGs have the same purpose: to make the complexities of on-line searching transparent to users. Virtually all commercial IG systems have one feature in common: automatic dialing and log-on to the search service. Command mapping is another important feature since it provides for language translation between different on-line systems. Many users want to capture the results of a search in one

on-line system and have them reformatted to become a query for another system. Some IGs automate the process of transferring data among systems. Downloading results for local manipulation, file merging, editing, accounting, and recordkeeping are other functions that most IGs support to some degree.

Off-line query definition and rapid execution of an on-line search are two cost-reduction features of IG systems. Since most on-line services charge for time instead of the value of a search, ways have been devised to reduce the amount of time spent connected to those services. The software on the user's microcomputer or intelligent terminal performs the search automatically, downloads the search results, and logs off. The user does not need to know many specifics about the search service command language, syntax, protocols, and so on; thus, the novice user can perform a search more easily.

By capturing the semantics of the underlying data, IGs can support powerful query facilities that allow a user to be selective about the data retrieved. In this way, the volume of data transmitted can be greatly reduced, easing the communications burden.

Research on gateways began in the mid-1970s, and operational systems became available in the early 1980s. The IG approaches discussed here are representative of the commercial and experimental efforts under way in the Federal sector and in private industry. For purposes of this report, the IG approaches have been categorized as basic gateway systems, interoperation gateway systems, and integration gateway systems. Appendix C presents a discussion of the major issues associated with interoperation and integration gateways, focusing on the semantics to provide integrated access to CALS data. These gateways are concerned with the preservation of the meaning of information as it is transferred from the sender to the recipient. Individual requirements determine which approach is best suited to a particular application. Appendix D presents a discussion of the functions and capabilities offered by the basic gateway systems mentioned in the following section and identifies two expert front-end systems that explore the use of artificial intelligence technology to provide user-friendly gateway front ends.

3.1 BASIC GATEWAY SYSTEMS

Basic gateway systems offer a comparatively inexpensive means for a user at a single terminal to access and retrieve data from heterogeneous sources. These

systems do not interface directly with DBMSs at the target host. Rather, they interface with programs that have been written at the target host to retrieve data from the local databases. The accessing gateway system is seen simply as another user by the target system. The gateway vendor does not know and has no need to know what type of hardware, operating system, DBMS, or other software is supported at the remote location. All the vendor has to know is that the data are to be sent in asynchronous, American Standard Code for Information Interchange (ASCII) format.

The basic gateway approach is the simplest to implement. User responses to system prompts are reformatted to be read by batch or interactive programs at the target computer system. In Appendix D, we describe the capabilities offered by four existing basic gateway systems: the Technical Information System (TIS) of Lawrence Livermore National Laboratory (LLNL); Knowledge Gateway Service (commercially known as EasyNet) of Telebase Systems, Inc.; IRVING Library Network of Minicomputer Systems, Inc.; and the Chemical Substances Information Network (CSIN) of the Computer Corporation of America (CCA). Three of these basic gateway systems offer the following capabilities needed to support a number of logistics operations in the near term:

- Transparent dial-up and log-on
- Menu-driven system for formulating user queries
- Software to determine which database(s) should be accessed
- Data retrieval and postprocessing.

(Only the CSIN does not provide all four capabilities.)

Any and all conversions (to ASCII and to accommodate record layout and data element format requirements) are handled by the gateway. The target computer system simply receives and processes the data sent by the gateway without knowing where the data originated.

The capabilities for database access and data manipulation provided by the currently available basic gateways are limited in the sense that the user is provided with only one of two means to access the data; once logged on to the remote system, the user must know the local commands to retrieve information or be satisfied with the information retrieved via predefined menus and prompts.

User-friendly features of basic gateway systems can aid the novice searcher and the casual or occasional searcher who does not wish to memorize the detailed specifications required for on-line searching. They may also aid the experienced user who is familiar with the terminology and contents of specific databases. On the other hand, basic gateway systems prevent the nonexpert user from reaping the benefits of the interactive aspect of the search service and the facility for iteratively developing and improving search strategies.

The basic gateway approach can be used to support a limited number of types of queries where the request is a standard, predefined query; only a few programs (batch or interactive) may have to be accessed at the target system; and only certain data elements must be accessed in the databases or files on the target host. In such cases, the users' questions and the responses to them are known in advance; and in such situations, the basic gateway approach could prove to be the most cost-effective. The basic gateway approach also allows the target host computer to control user access to its data more easily. Today, the basic gateway concept has a wide range of uses in the logistics community; for certain applications, it is a concept that could prove to be the long-range solution.

3.2 INTEROPERATION AND INTEGRATION GATEWAY SYSTEMS

This section presents an overview of the issues associated with providing integrated access to a heterogeneous collection of technical information supporting a variety of different applications. These issues (addressed more fully in Appendix C) arise when the basic gateway facilities are augmented with the ability to access the underlying systems in an ad hoc fashion as though they were a single integrated database.

A general solution to the problem is technically difficult and not within the capabilities of current technology. However, we have examined CALS objectives to identify approaches for providing many of the required capabilities. One approach that can be pursued with current technology is that of interoperation gateways, where "global" facilities are provided to support the *illusion* of integration among potentially autonomous, heterogeneous systems. A longer term approach, integration gateways, would provide facilities to access technical information in diverse, specialized repositories and to support control of that information.

The issues addressed correspond to support for *meaningful use* of data in the context of a target application. The OSI reference model is concerned with the preservation of information as it is transferred from the sender to the recipient (OSI Layer 6) and with those aspects of the information exchange that are visible to the applications, such as identifying the communications partners (OSI Layer 7). In fact, the functions in Layers 6 and 7 support only part of the CALS data access and integration requirements because access to information, particularly information from heterogeneous sources, requires more than the concept of system interconnection as expressed by the reference model.

This section is concerned with those issues associated with OSI Layers 6 and 7 and with issues of preserving the meaning of the data and providing their logical (but not necessarily physical) integration, i.e., giving the illusion of an integrated database without requiring changes to the underlying databases. While the issues involve both technical and management concerns, this document focuses only on the *technical issues* associated with providing access to heterogeneous sources and integrating information from them. We consider management issues to the extent that they will need automated support since providing such support may pose additional technical problems.

3.2.1 CALS Requirements and Issues

The following are the primary requirements of CALS:

- Maintaining weapon systems configuration data electronically and in near real-time
- Storing, retrieving, distributing, and processing electronic logistics technical information
- Integrating logistics technical information from a variety of data sources
- Integrating design and design analysis processes, with focus on reliability and maintainability (R&M)
- Interfacing with manufacturing systems for competitive parts production with significantly reduced leadtimes
- Providing end users with transparent access to distributed logistics technical data.

Those requirements presuppose access to technical and engineering information at different physical locations and across the boundaries of individual applications and even organizations. The requirements focus specifically on data *access* and *integration*. Providing that access and integration poses many technical, managerial, and legal problems for several reasons:

- The data recipients operate in different environments from the data sources or suppliers; they support applications that serve specific engineering or managerial purposes; and they may perform their functions autonomously.
- Integrating information across processing environments raises issues about the usefulness of that information outside its original environment and also with the management of the integration process.
- The use of information outside the original environment raises such legal issues as the protection of proprietary information, trade secrets, copyrights, etc., and the liability for accuracy, correctness, and currency of the information.

In the long term, CALS must provide integrated access to information across different physical locations, across application boundaries, and across organizations. Issues will arise not only in the context of agreements between two applications, but also in the selection of sources to provide the required information and in the interpretation and combination of data across multiple sources. In order to provide integrated access to information, CALS must address the problems of where to get the information, how to get it, and how to use it.

3.2.2 Survey of Efforts to Develop Logical Integration Services

Several organizations are currently at work on facilities to provide integrating services across heterogeneous distributed databases. Much of that work is in the early stages. Research projects are addressing such issues as distributed DBMS technology; incompatibility resolution and composition of data from distributed, heterogeneous sources; and view integration and database design. Research should also address high-level semantic issues that could provide integration.

Although some commercial systems have begun to provide facilities for supporting access to heterogeneous databases, [e.g., the Design Automation Standards Subcommittee (DASS) supports joining data from different databases based on common names and the distributed Interactive Graphics and Retrieval System (INGRES) and distributed ORACLE will provide some support for access to

heterogeneous systems], in general, commercial systems place too many restrictions on the degrees and types of heterogeneity allowed in the underlying systems and databases to be of real value to CALS.

On the other hand, the issues discussed in Appendix C are the focus of several research-oriented prototype efforts. The Institut National de Recherche en Informatique et en Automatique (INRIA) in France has prototyped the MULTICS Relational Data Store Multidatabase (MRDSM), a "multidatabase" system for simultaneously accessing several relational databases by dealing with incompatible names, values, and meanings. NASA is currently developing DAVID, which has focused on language and model mapping issues. Other work on integrating heterogeneous databases is being pursued at Honeywell and at the Microelectronics and Computer Technology Corporation (MCC). The Computer Corporation of America (CCA) MULTIBASE prototype provides an integrated view over disparate systems that range from file servers to DBMSs. Continuing research on the CCA PROBE project focuses on data modeling issues and addresses the use of an object-oriented approach to distributed data access and integrating special-purpose processors.

Other projects are exploring not only the issues involved in how to build a gateway but also the role of gateway architectures in addressing specific applications problems. They are developing target architecture approaches that are similar to those required by CALS. The Integrated Design Support (IDS) project at Rockwell International is developing an architecture for integrated access to contractor- and subcontractor-maintained aircraft engineering and manufacturing life-cycle data. In IDS, MULTIBASE is being used to demonstrate gateway functionality. The Very High Speed Integrated Circuit (VHSIC) Executive Information System (EIS) program is developing a set of software and standards to facilitate distributed sharing of integrated circuit design data within and among VHSIC design organizations.

3.2.3 Interoperation and Integration Gateways for CALS

Appendix C presents two views of CALS data access and integration requirements: an "external" (or end-user) view of required capabilities and an "internal" view of required facilities, i.e., of system requirements implied by the external view. The appendix also discusses the key issues raised by the required capabilities and

outlines technical approaches that can provide the means for addressing many of these issues.

Appendix C summarizes a plan for pursuing the long-term technical approaches for integration gateways. The plan reflects the goals of *reusability* and *leveraging* on the results of the research efforts and research-oriented prototypes cited in Section 3.2.2. The key to implementing IG services for CALS is to use current technology to address immediate data access needs and to prototype and incorporate advanced technology as it becomes available. Appendix E surveys standards relevant to any CALS IG effort.

3.3 EXPERT FRONT-END SYSTEMS

Artificial intelligence techniques and specialized expert systems are being applied to the area of transparent systems for aiding on-line database searching and the development of user-friendly interfaces. Expert front-end systems attempt to use artificial intelligence techniques to interpret a user's question, to make a judgment about what the user really means, and to put the question in the format and language that a particular search system requires so that the right answers are retrieved. Some gateway services choose the database for the user based on the type of questions the user asks. Although those systems often claim to choose the "best" database for a search, they may not always do so.

Search strategy formulation and refinement for database systems is a sophisticated feature not widely available, albeit much needed. Artificial intelligence has been successfully applied in some systems, particularly in the field of medicine, but no available expert system does a good job of addressing the problems of on-line searching.

Two current development efforts seek to provide a more sophisticated expert front end. They are the Front End for Databases (FRED) project at General Telephone and Electronics (GTE) Laboratories, Inc., in Massachusetts and the Connector for Networked Information Transfer (CONIT) project at the Massachusetts Institute of Technology (MIT). The two expert front-end systems are experimental and use techniques of artificial intelligence in the development of a natural language, dialog-based user interface. These systems address the need to assist the user in search strategy formulation and refinement, which is basic to bibliographic types of data

retrieval. However, the techniques being developed could very well be applied to data retrieval in support of acquisition and logistics operations.

Both CONIT and FRED provide the user with a transparent log-on capability; both are menu-driven with the additional natural language-like processes to help the user formulate more effective queries; and both automatically perform searches across multiple databases based on a single user query. That technology would be useful as a front-end extension to any gateway approach.

3.4 COMPARISON OF APPROACHES

All the systems described thus far in Section 3 have been developed to provide an integrated interface, or gateway, between heterogeneous databases. However, significant differences exist among the approaches used.

In general, four approaches have been used to implement the user interface. The simplest are those used by TIS, EasyNet, IRVING, and CSIN, which provide menu-driven selections to the users. The TIS provides a menu-driven system that supports transparent dial-up and log-on procedures. However, the user must be familiar with the selected resource since search negotiations must proceed according to the syntax and logic of the target system. EasyNet's menu-driven user interface is well suited for simple searches, and users generally develop their own downloading and postprocessing routines.

The IRVING system allows a user to operate in either of two modes. In the "transparent" mode, the full range of the target host functions is available to the user. The user can also operate in "network" mode, which provides a menu-driven capability for bibliographic searches. CSIN offers three modes of operation: direct use, for which the user must know the details of using the remote system; enhanced direct use, which can send prestored message sequences to the remote system, transform data received, and send transformed data to other systems; and script use mode, in which a prestored script (program) mediates between the user and a number of remote systems. Of these four approaches, CSIN appears to offer the most complete user interface.

Interoperation gateways, such as MULTIBASE, are designed to accept more of the data access burden, transparent to the user. In adopting a retrieval language and data model that can handle complex queries against any style of DBMS, the user

perspective of the gateway is often more complicated than that of a basic gateway. However, part of the evolution of these systems involves experimentation with more "friendly" intelligent front ends.

The interoperation and integration gateway environments include special data dictionaries to handle the distributed, heterogeneous data management problem. Existing commercial data dictionaries are unable to handle physical distribution of the data in integrated DBMSs. The data dictionary being developed in each interoperation gateway effort is a database that describes shared data (the conceptual schema), the characteristics of local databases and DBMS software, and the network environment. Processor software accesses the data dictionary and transforms user data requests from a common query language into transactions that can be processed by the local DBMSs and file systems. The result is a need for a total of 2N translators (where N is the number of different underlying DBMSs or file systems) rather than (N-1)N translators, as required in the current commercial data dictionary approach.

Integration gateways provide access to and support for control over technical and management databases by integrating the specialized hardware and software facilities that store and manipulate these data types, such as text or two-dimensional or three-dimensional graphics. These gateways rely on powerful data models to capture more of the semantics of technical information than can be captured by simpler gateway systems. In this way, they can support more sophisticated or specialized operations over the information than retrievals based on index terms or simple transfer. Examples of these operations would include spatial searches on graphical data, proximity searches on text, or change control procedures over distributed, heterogeneous repositories and technical data types. PROBE, which is based on an object-oriented data model, is an example of an experimental offer to develop this type of gateway.

Table 3-1 summarizes the various facilities available on each of the example systems. One characteristic shown in that table is the ability to search multiple databases. That characteristic is a reference to the system's ability to automatically interrogate multiple databases to satisfy a particular query. This "intelligent" search procedure would present the user with the final result without requiring user intervention before each database is queried.

TABLE 3-1

INTELLIGENT GATEWAY FACILITIES

Characteristic	TIS	EasyNet	IRVING	CSIN	MULTIBASE	PROBE	Intelligent user interfaces
							CONIT/FRED
Existing applications	Biblio	Biblio	Library	Chemical biblio	General purpose	General purpose	Biblio
Extensibility	None	None	None	None	Building blocks provided	Built-in	N/A
Automatic dialing and log-on	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access language	None[a]	Menus/prompts	Menus/prompts	Menus/prompts	Query language	Query language + user-specified operations	Natural language
Access multiple DBMSs	No	Planned	No	Yes	Yes	Yes	N/A
Support for technical data[b]	No	No	No	No	No	Yes	No
Update facilities	No	No	No	No	Planned	Yes	No
Management support[c]	No	No	No	No	No	Yes	No
Status/availability	Product	Product	Product	Service	Prototype	Experimental	Prototype

Note N/A = not applicable

[a] User must know target system access languages

[b] Proximity searching within textual and graphical data

[c] Facilities to support versioning, configuration management, change control, etc

Another important consideration is the power of the user interface facilities. The most sophisticated approach is the natural language dialog between the user and system available from CONIT and FRED. Variations exist in the level of sophistication of the natural language inputs, the quality of system response, and the level of user assistance provided. Both systems apply artificial intelligence technology in the development of their natural language dialog-based user interfaces. Such "front-end" systems are appropriate for use with any of the classes of IGs.

Hardware and software availability should also play an important role in the selection of a system. Several of the systems examined have not been completed; some exist only in prototype, while others are still experimental.

3.5 CALS INTELLIGENT GATEWAY DEVELOPMENT

The plan for developing IG capabilities for CALS has three primary goals: reusability, leveraging, and transition. *Reusability* ensures software modules, modeling activities, and designs developed in the near term are augmented rather than replaced by subsequent gateway development activities. *Leveraging* other Government-sponsored projects that are pursuing related activities ensures CALS activities in all phases build upon existing work to the extent possible. Providing a smooth *transition* from simple to very powerful gateway capabilities ensures the continuous availability of gateway services as CALS progresses from basic through interoperation and ultimately to integration gateway facilities.

In order to allow for smooth migration to OSI, a CALS IG architecture should separate the communications functions from the data interchange formats, intelligent data presentation management, data dictionary, and user interface (or query) functions. This distinction will ease the interoperation of systems during the DoD-to-OSI protocol transition and will also simplify the implementation of dual protocol gateways.

Several Government-sponsored projects may develop designs or software modules that can provide CALS IG services. For example, the IDS project at Rockwell International, which focuses on information and process modeling for document control, can provide application models as well as high-level gateway architectural concepts. The VHSIC EIS project, which is designing and building an object-oriented *environment* that is essentially a tailorable IG, may provide facilities to support management and control and direct support for technical data. Other

projects, noted in earlier sections, are specifically developing IG services; they may provide software that can be used directly as baseline CALS gateway functionality.

This telecommunications plan is based on a model of the target CALS IG architecture, which is described in detail in Appendix C. That architecture views a gateway as a framework of standards and services, which together provide end users and application programs with transparent access to distributed heterogeneous repositories of technical data. The gateway *standards* describe the user's view (model) of the system and define the mappings to be supported between gateway protocols/standards and the underlying systems (see Figure 3-1). The gateway functionality is provided as a network of *services*, in which supporting services are invoked as necessary (see Figure 3-2).

In this plan, we assume that telecommunications facilities (often referred to as "communications gateways") will be available to interconnect the underlying host systems. In each of the three phases of the plan – the near-term, mid-term, and long-term phases – a collection of design and development activities will result in incremental IG capability and in concurrent standards development, modeling, prototyping, and experimental activities that will serve as the basis for subsequent efforts.

3.5.1 Near-Term Gateway Activities

The goals of the near-term activities are to provide basic gateway services and to lay the groundwork for more powerful mid- and long-term gateway services. In this phase, CALS project managers must perform the following primary activities:

- Identify and adopt gateway standards
- Acquire and install basic gateway software
- Develop and document application-specific models of logistics information over which IG services can operate
- Establish requirements for interoperation gateway services and develop and document operational concepts for such services, along with plans for building on those concepts to produce, in the long term, integration gateways
- Begin the software development or enhancements of existing prototype or experimental software that will form the basis of mid- and long-term gateway services.

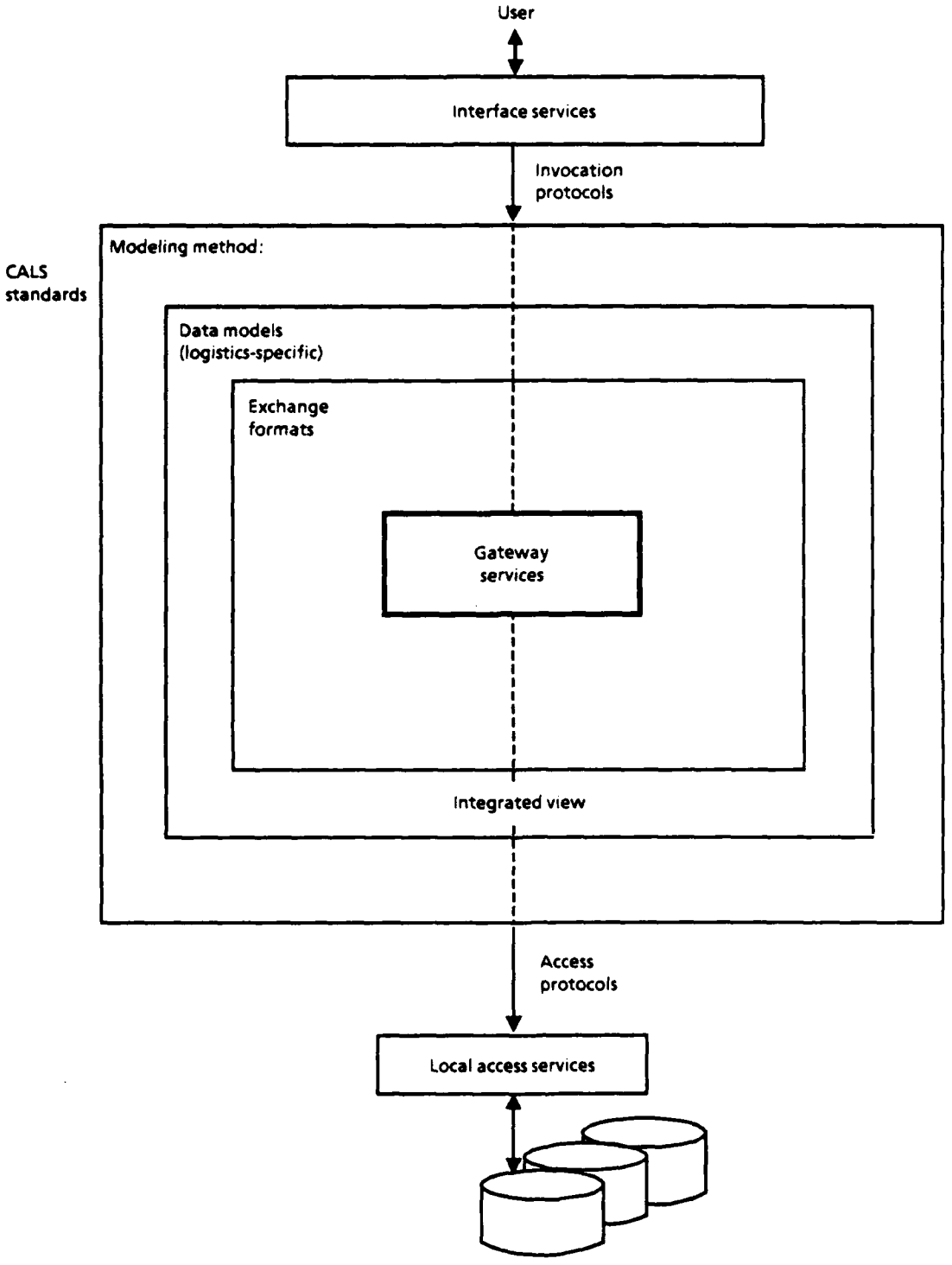
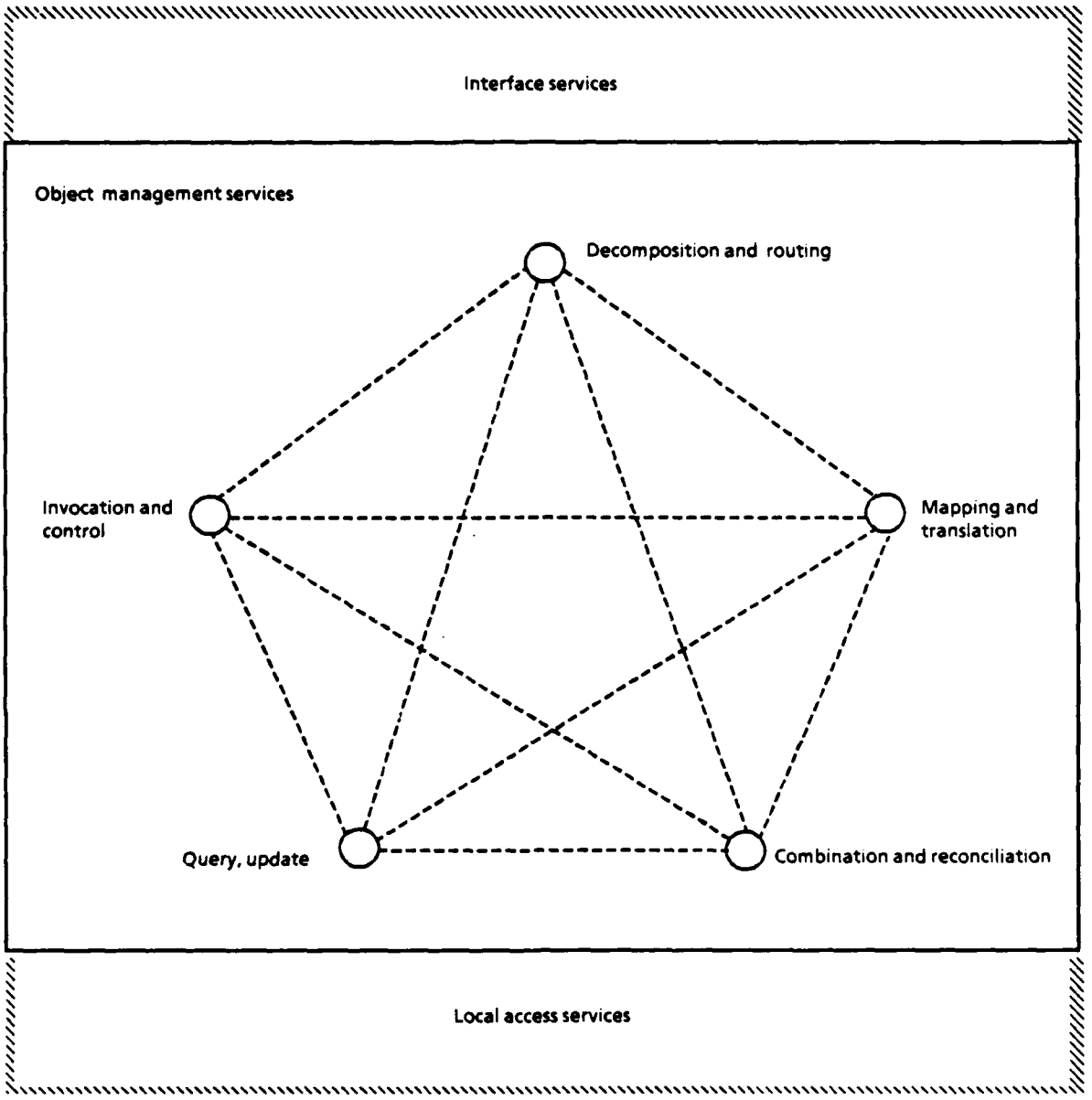


FIG. 3-1. STANDARDS ARCHITECTURE (LONG-TERM TARGET)



Services architecture (long-term target)

- Object-oriented
- Loose federation
- Distributed

FIG. 3-2. SERVICES ARCHITECTURE (LONG-TERM TARGET)

The information modeling tasks performed in this phase should include defining the requirements for supporting access to technical information, specifically as those requirements affect selection of a modeling method and design of dictionary and directory structures. Existing standards used to define technical data, including the Product Definition Exchange Specification (PDES) and the ICAM[1] Definition (IDEF), may levy additional requirements. Supporting tasks include cataloging existing application databases and defining for each the objects, operations, constraints, and inter and intradatabase dependencies on which change control procedures will be based.

The software development and enhancement tasks performed in this phase should include initiating development of a minimal set of interoperation gateway functions and prototyping selected long-term capabilities. For example, MULTIBASE or other gateways might provide baseline interoperation gateway modules. PROBE provides some intelligent processing facilities that could be used to prototype special processing for CALS-specific data types.

3.5.2 Mid-Term Gateway Activities

The goals of the mid-term activities are to implement CALS interoperation gateway services and to continue the design and prototype of long-term capabilities. The primary activities of this phase are as follows:

- Implement and demonstrate the selected set of CALS interoperation gateway services initiated in the near term
- Identify and incorporate enhancements to the baseline CALS interoperation gateway functionality
- Refine the requirements for an integration gateway prototype and the plans for transitioning from the interoperation gateway environment.

Implementation of the interoperation gateway services must be supported by application-specific efforts, including database design and schema specification. A full demonstration of the gateway services should be planned.

Possible enhancements to the CALS baseline interoperation gateway functionality include single-site update and data administration services, including support

[1]Integrated Computer Assisted Manufacturing.

for dictionary design and schema management. In addition, extending the interoperation gateway functionality to support a full object model would position CALS for transition to the long-term scenario. Integration gateway activities include continued prototyping efforts, including user interfaces, leading toward a full *prototype* demonstration of the CALS integration gateway concept.

3.5.3 Long-Term Gateway Activities

Successful CALS implementation will hinge on further IG studies and development. These efforts should focus on activities that will

- Establish the requirements for and scope of global guidelines and standards
- Identify technologies that will influence the role and nature of gateways in the long term
- Define the long-term requirements and technical approaches for and architecture of a global logistics support and information system
- Determine the functions and generic components that should be provided or promoted by a global authority, and identify long-term technical approaches and candidate technologies for providing them in a cost-effective manner
- Produce specifications for a long-range research and development program that focuses on the application of relevant technologies to specific CALS issues.

The following list summarizes eight recommended tasks and their interrelationships.

Task 1 – High-Level Analysis of Long-Term Goals. This task would create a high-level model of a future logistics support and information system, describing target capabilities, scenarios for end-user interactions, and requirements for functions and specifications that transcend individual logistics support systems.

Task 2 – Detailed Studies of Key Technical Areas. This task would refine the understanding of technical requirements and approaches in key areas of global support functions. These include four principal areas:

- Gateway services
- User interfaces

- Management and control
- Data access and integration.

Task 3 – Long-Term Architecture and Plan. This task would integrate the results of previous activities. It would (1) produce a target architecture that supports CALS long-term objectives, (2) identify its components and needed interfaces, and (3) recommend technical approaches for their implementation. In addition, it would produce a plan for a first phase of tasks intended to support realization of and transition to the long-term goal.

Task 4 – Information Modeling Study. This task would examine the long-term prospect of standard specifications that CALS would require in many areas. It would use information developed during Tasks 2 and 3 regarding the key areas in which such specifications are needed and the functions they would have to serve.

Task 5 – Intelligent Gateway Studies. This task comprises a family of activities that would determine and design gateways on OSI Layers 6 and above for a variety of future global CALS services.

Task 6 – Core Information Model Requirements. This task would formulate requirements for a core model of information (and processes) that would serve the long-range CALS need for flexible standards, transformation of technical information to suit requirements of individual application environments, etc. It would serve the Government's need for identifying long-term requirements for and approaches to CALS-related standard specifications.

Task 7 – System Standards. The objective of this task would be to define a set of target specifications (including interface standards) for a long-term CALS system. The specifications would support the integration of the services needed to support the target system defined by Task 3.

Task 8 – Security Requirements. This task would be a study of the security policy implications of the long-term CALS system, and a definition of security support functions that might have to be provided by the long-term system.

The goal of the long-term activities is to transition from interoperation gateway services to integration gateway services. The activities include using the prototyping efforts to feed design and development of production-quality integration gateway

capabilities and effecting the transition. Figures 3-3 and 3-4 depict a high-level architectural view of this transition.

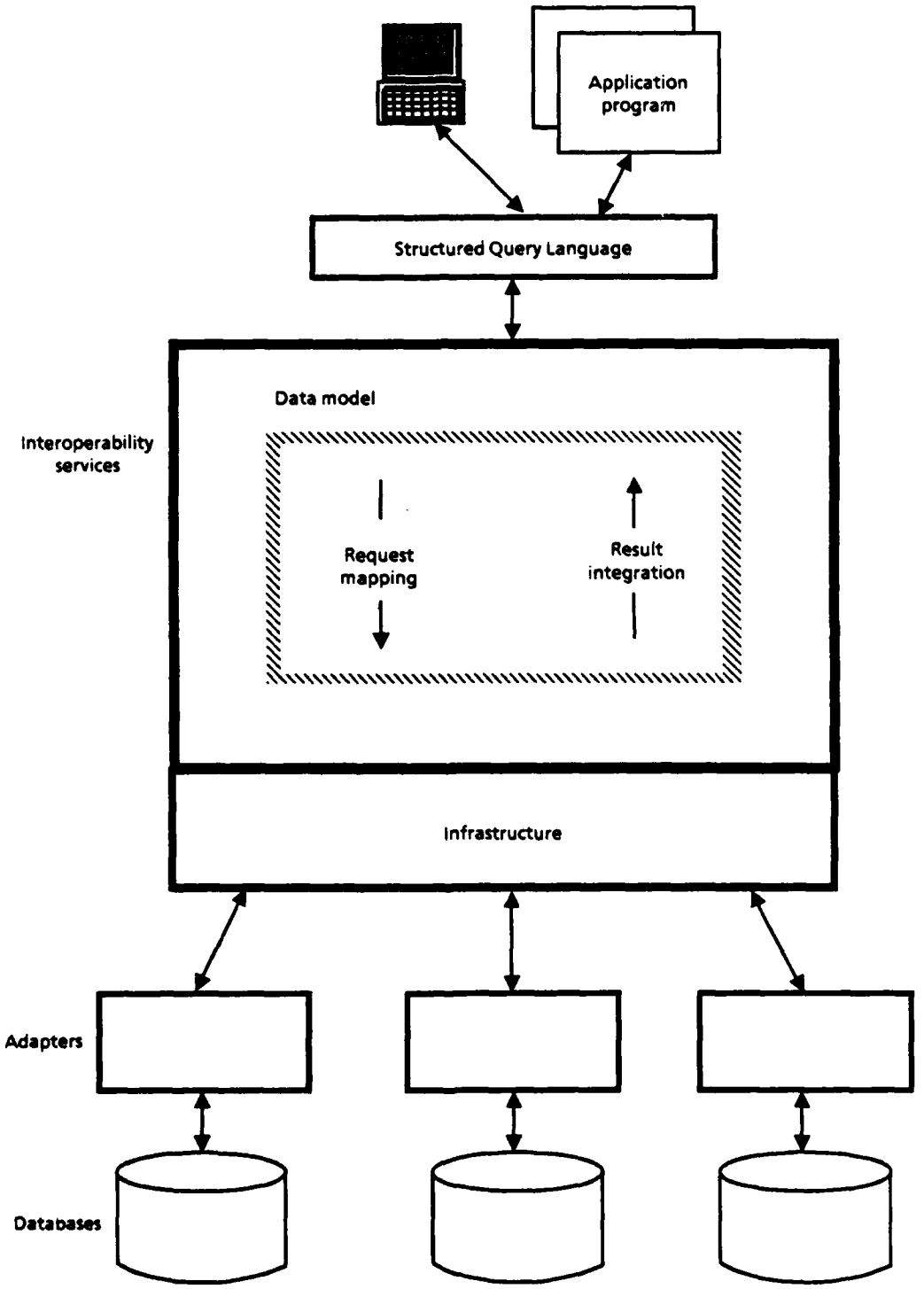


FIG. 3-3. INTEROPERATION GATEWAY (INTERMEDIATE CAPABILITY)

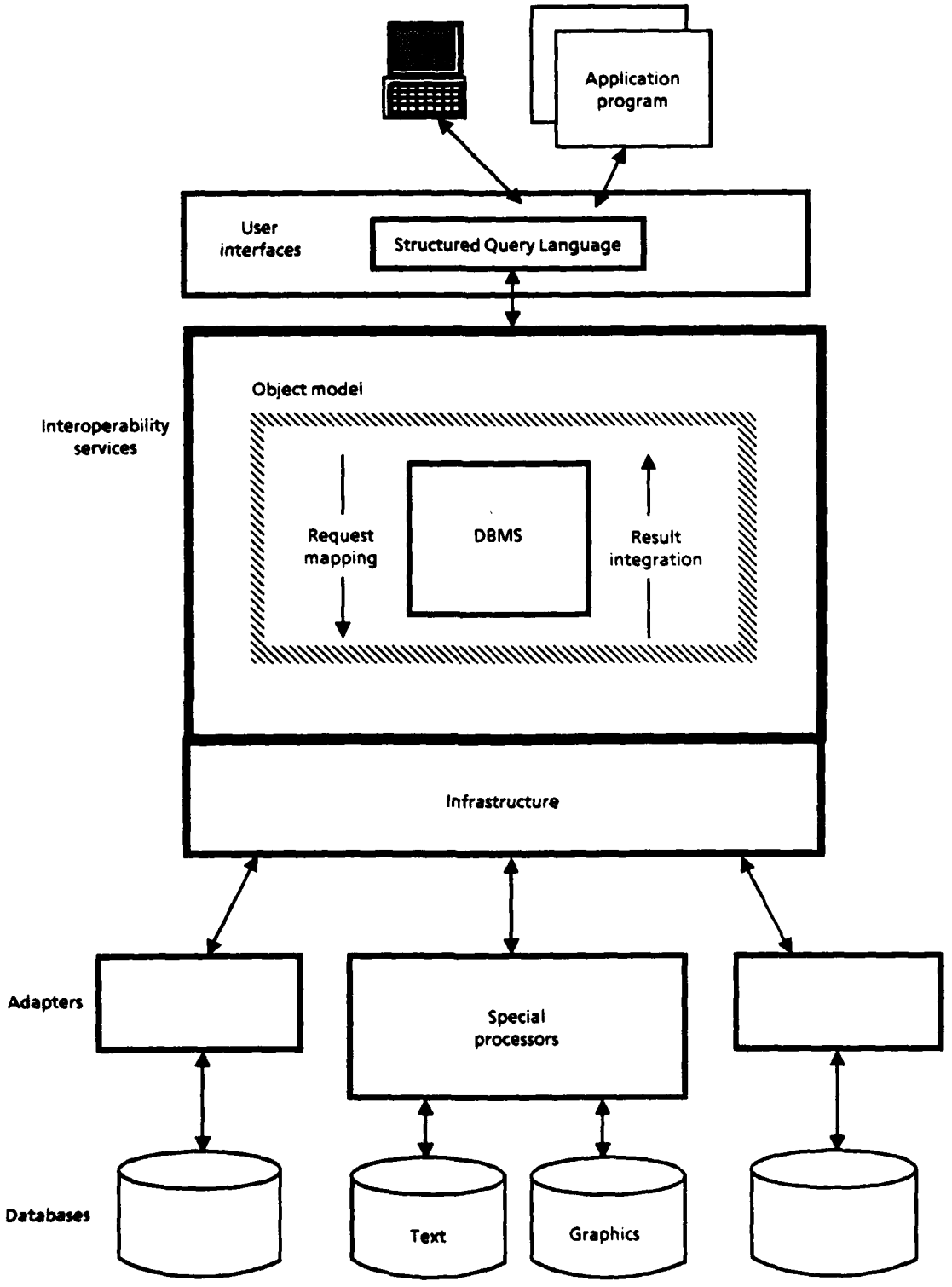


FIG. 3-4. INTEGRATION GATEWAY (TARGET CAPABILITY)

SECTION 4

COMMUNICATIONS SECURITY AND RELATED ISSUES – A MANAGEMENT PERSPECTIVE

The CALS goal is to provide a highly automated, functionally integrated capability for generating and processing acquisition and logistics support information. That goal is to be achieved by affording users real-time, on-line, transparent access to needed logistics support data through networking of automated logistics support databases.

CALS will span the program life cycle of weapon systems from preconcept planning through development and support to product disposal, and it will be implemented across all weapon systems and throughout DoD.

Weapon system contractors and subcontractors, as sources of design-related logistics technical information, will interface with DoD systems and users to exchange information electronically. This electronic, paperless data access and distribution capability will greatly improve the timeliness and accuracy of technical information and will also pose new problems and risks in terms of security, data integrity, and data and software ownership.

Congress passed the Computer Security Act of 1987 [Public Law (P.L.) 100-235] which assigned the responsibility for the development of security standards and guidance for the protection of unclassified data to NIST. Classified data remain the responsibility of NSA.

While the majority of data in any CALS network will be unclassified, they will also be sensitive. At some threshold the aggregation of this unclassified but sensitive information may result in classified information, and that information falls into the joint domain of NIST and NSA.

Since a significant amount of sensitive data is exchanged among DoD components and between DoD and industry, a low-cost means of protecting those data is essential. Additionally, that protection must be developed in such a way that it can

be integrated with higher security levels to provide a seamless multilevel security system.

The CALS telecommunications architecture presented in Section 2 addresses security from a technical perspective. In this section, the legislative and management issues of data and software security are addressed. The subsequent sections provide some background on data and software security and then discuss the following topics:

- Legislation and DoD policy issues related to CALS, including the following:
  - DoD "Sensitive but Unclassified" data issue
  - National-security-related computer crime legislation, including unauthorized access to computers supporting the Government and interception of electronic mail communications
- DoD technical data and software ownership policy issues
- Issues of data integrity and accuracy in the decision-making process
- Copyright issues associated with the protection of copyrighted software accessible through LANs or other communications media.

In the final section, we present a discussion of additional network security technology that is commercially available or under development and the importance of security standards. We emphasize the manager's role in ensuring security protection within an organization.

4.1 BACKGROUND

The basic policy document for Government-wide information security is Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, issued in December 1985 (replacing Circular A-71, *Transmittal Memorandum No. 1*, issued in 1978). Circular A-130 requires agencies to designate security officers, conduct risk analyses, and take other appropriate steps to protect their information systems. Between 1 January 1978 and 31 March 1982, 172 cases of computer-related fraud and abuse were found in just 12 Government departments and agencies, and half of those incidents were detected solely by accident. The high proportion of cases detected by accident is alarming because of the implication of weaknesses in internal controls and the potential for undetected fraud and abuse.

CALS implementations face fundamentally new levels of risk in information security because of increased use of networks (both LANs and WANs), increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, the rapid growth of dial-up facilities, and increased dependence on information technology.

Most mainframe computers are now part of a LAN or a WAN. Office automation systems and Ethernet-like connections provide easy access to data and present an increased risk since, in many configurations, users have access to all databases on the network. The same technology used in many IG development efforts today can be used to program a computer to automatically tap into other databases or store downloaded data with no need for any direct human intervention.

Vulnerable components of a network include the physical links that carry the information (such as dedicated lines, telephone dial-up lines, microwave, satellite, and LANs) and the points or nodes at which the information is switched from one communications path to another. Connections between networks are not always visible. Since it is possible to hop from one network to another, a user's path is virtually impossible to trace. Today, more than 150 networks have legitimate connections to the DoD's Military Network (MILNET) and the (Defense) Advanced Research Projects Agency Network (ARPANET).

The CALS network must anticipate threats from multiple sources with various intents. The most likely threat is not from outsiders (who typically comprise only a small fraction of data security problems) but from dishonest or disgruntled employees with authorized access. Actions of these individuals can be damaging but are usually unsophisticated and can be largely countered with good security procedures. Nonetheless, the CALS network must be robust enough to withstand more deliberate threats by hostile entities. Because it will contain industry-proprietary data, the CALS network is a potential target for industrial espionage both from outside interests and from CALS participants. A further concern is protection of the data from foreign intelligence collectors. Additionally, since the CALS network is important to national defense, hostile attempts to degrade the network through the use of worm/virus programs must be prevented. Just as jamming of communications systems is a threat to some military systems, so, too, are computer viruses a threat to

computer networks. Both can destroy information already in the system and prevent its further use.

Access to logistics databases must be limited to those that have need and have been specifically approved by the organization that owns the data and by the organization that manages the data. Contractors must be in a position to commit proprietary data to these databases with the assurance that their rights will not be compromised.

In a 1985 survey, the congressional Office of Technology Assessment (OTA) found that agencies often do not implement the security measures mandated or suggested under prior policy guidance. The OTA study identified three key factors inhibiting appropriate Federal information security measures: (1) competition for resources in Federal programs, which limits spending for a "latent" issue such as security; (2) a lack of awareness or motivation among agency personnel and top management; and (3) an absence of clear guidance on appropriate security measures.

Several CALS prototype efforts are under way or planned as are production development efforts. In addition to developing an overall security policy document for an organization, a security requirements analysis should be performed upon the implementation of any and all programs. A *network security architecture* should be developed along with the overall network architecture.

A network security architecture constitutes an overall plan and policy for the security of the system. Various security services will have to be implemented in the architecture to protect unclassified but sensitive data in an OSI environment. These services and their functions are listed below:

- *Access control* monitors unauthorized use or misuse of resources accessible by the network.
- *Data confidentiality* ensures either part or all of a certain data resource is protected from disclosure to unauthorized individuals or processes. Traffic flow confidentiality, which is related, protects data in transit to ensure no intelligence can be derived from observation of traffic flows.
- *Data integrity* prevents the unauthorized modification of data resources or, failing to do so, ensures detection of such unauthorized modification is possible.
- *Nonrepudiation* provides proof of delivery to the sender and proof of origin to the recipient in data transmittals. Also known as digital personal signature,

this capability provides proof of signature to third parties involved in resolving data delivery disputes. This service will be particularly applicable in CALS contractual matters.

- *Authentication* will ensure the identities of mutually communicating network entities in a connection-oriented environment. In a connectionless environment, authentication will ensure the claimed origin of data.

Network security architecture relates to the network architecture by identifying how the security services map onto the layers of the architecture. Placement of a particular service within a specific layer has far-reaching implications about the nature and extent of the service implementation. Since the services at one layer employ services at a lower layer, the exact nature of the functions provided in each layer affects the total service provided by the network.

4.2 LEGISLATION AND DoD POLICY RELEVANT TO CALS

4.2.1 The "Sensitive But Unclassified" Issue

The concept underlying the CALS program is to use advanced distributed data processing and telecommunications to integrate databases and processes supporting weapon systems. Some of the data may be classified and some may be unclassified but proprietary. Furthermore, some data that may be unclassified when considered at the data-element level would become classified when aggregated at the weapon system level. In any case, OSD needs to impose controls over who has authority to change, update, or release the data.

The electronic format makes possible rapid and extensive searches of large bodies of data that would otherwise consume significant time and expensive library research effort. With today's sophisticated software, analysts can search and organize data to create information that could become proprietary, or "controlled," information. At the same time, the very same information in print might well remain unrestricted.

The Computer Security Act of 1987 assigned to NIST the specific responsibility to develop standards and guidelines for Federal computer systems, including the responsibility for standards and guidelines to protect sensitive information in Federal computer systems. In this work, NSA can provide NIST with technical advice, assistance, and products. The term sensitive information refers to any information whose loss, misuse, or unauthorized access or modification could

adversely affect the national interest of the United States but that has not been specifically authorized under the criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy.

Many CALS programs are in the process of automating what are predominantly manual operations today. As part of the process of deciding which data in support of a weapon system should be maintained in databases for on-line access, data should also be reviewed for a possible "sensitive" classification.

NSA's National Computer Security Center (NCSC) and the National Telecommunications and Information Systems Security Committee (NTISSC) are working on a variety of schemes to categorize the sensitivity of unclassified national-security-related information and, ultimately, to specify appropriate security measures for each level of sensitivity. In related work, the NCSC has already developed a scheme for categorizing the technical security features of computer systems, ranging from those that require little more than password control (the "C1" level) to those whose operating systems can pass sophisticated tests of design integrity (the "A1" level) in the Department of Defense Trusted Computer System Evaluation Criteria, or the *Orange Book*. The NCSC has an ongoing program for evaluating products submitted by vendors in order to rank them according to their technical security-related features.

4.2.2 National-Security-Related Statutes

Some specialized statutes relate to national security; among them are Sections 793 – 795, 797 – 799, and 952 of Title 18 of the United States Code (U.S.C.). The broadest, Section 793(f), covers virtually all misconduct having to do with information or documents related to national security, including the knowing failure to report the loss of such documents. Computers compound the problem of missing documents because it is difficult to tell whether a file has been copied by an unauthorized person if the file is not missing or, if it is missing, whether its loss is the result of a computer malfunction, a user error, or a criminal act.

In October 1984, Congress enacted the first Federal criminal code provision dealing specifically with computer crime. That legislation deals with three distinct forms of computer abuse, two of which are relevant to DoD. First, the Federal Computer Crime Act deals with computer abuse involving national security issues. Specifically, Section 1030(a)(1) makes it a crime to access a computer without

authorization (or to use a computer beyond authorization) to obtain information falling within specified security categories with the intent to use such information "to the injury of the United States or to the advantage of any foreign government." (Even if no intent exists, a crime is committed if the unauthorized accesser should know that the information will injure the United States.) This offense is a felony punishable by up to 10 years in prison and a $10,000 fine.

The second type of computer abuse covered is the use, modification, destruction, or disclosure of information in a computer system accessed without authorization or used beyond the purposes of the authorized access. These activities are criminal only if they occur in a computer "operated for or on behalf of the Government of the United States." Furthermore, the activity is criminal only if it "affects" the Governmental operation of the computer. This offense is punishable by up to 1 year in prison.

The Electronic Communications Privacy Act amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968 – the Federal wiretap law – to protect against the unauthorized interception of electronic communications. In an electronic mail system, a message must be protected while it is stored in the user's electronic mailbox or in the system operator's computer and while it is being transmitted over telephone lines to and from the computer. The act includes a provision that prohibits employees of service providers from divulging the contents of any communications that they might inadvertently become aware of. However, it does not protect stored data that are not associated with an electronic mail or communications system.

Electronic mail systems are widely operated by industry and Government agencies for their own internal use. During the next decade these various discrete systems will increasingly interconnect with each other. For example, electronic mail systems may be used in CALS programs to transmit management reports from industry to DoD and among DoD organizations. Electronic mail users deserve privacy protection regardless of what type of entity runs their system or the system they use to reach a message recipient.

4.3 TECHNICAL DATA OWNERSHIP, RESPONSIBILITIES, AND PROTECTION

The more widespread data access becomes, the more crucial questions of data ownership, responsibility, authority for change, and secondary data uses become. Industry recognizes and is concerned that emerging automation technology may outpace the changes in contracting procedures and management processes required

to take advantage of EDI. Use of electronic data and computer technology will affect the structure of the defense industry and the relationships among its various segments. Industry support for CALS depends on a balanced approach that rewards innovation and, at the same time, makes the appropriate data available for competitive purposes.

The President's Blue Ribbon Commission on Defense Management (The Packard Commission) includes in its report a discussion on DoD and rights in technical data. The report points out the heavy emphasis in DoD on receiving unlimited rights in technical data on proprietary items so that other firms can use those data to compete with the firm providing the data.

Earlier, two nearly identical laws covering technical data acquisition and rights were enacted. One, the Small Business and Federal Procurement Competition Enhancement Act of 1984, P.L. 98-577, dealt with the technical data aspects of civil agency procurement; the other, the Defense Procurement Reform Act of 1984, P.L. 98-525, related to DoD procurements. Both acts required the promulgation of regulations concerning technical data acquisition and rights as a part of the Federal Acquisition Regulation (FAR) System.

The two statutes differed in some respects and it was feared that this left the way open for widely divergent interpretations and would result in unnecessary confusion, delay in implementation, and lack of uniformity. The Packard Report, therefore, recommends enactment of a single statute covering technical data or, if dual statutes are required in this area, that they be identical.

The Packard Report recommends that the Executive Branch develop an overall technical data rights policy embracing the following principles:

- Except for data needed for O&M, the Government should not, as a precondition for buying the product, acquire unlimited rights in data on commercial products or products developed exclusively at private expense. The Government should select the rights least obtrusive to the private developer's proprietary position.
- The Government should encourage a combination of private and Government funding in the development of products. Whenever practicable, the rights of the parties should be established before contract award.
- If products are developed exclusively with Government funding, the contractor/developer should be permitted to retain a proprietary position in the

technical data not required to be delivered under the contract or delivered but not needed by the Government for competition, publication, or other public release. Use by or for the Government should be without additional payment to the contractor/developer.

4.3.1 Data Integrity

The DoD must develop clear guidelines delineating responsibilities for maintaining logistics support analysis record (LSAR) databases. Today, each of the various requiring activities and associated contractor organizations maintains its own databases with little or no coordination among them. As a result, at any given time, no two Defense activities are operating from the same data. In addition, once the system has been fielded, no single agency is responsible for delivering, accepting, maintaining, and preserving the system's LSAR database. Complete and up-to-date information is essential to life-cycle support of a system/program.

Effective influence on the equipment design process requires the development of either interactive techniques or a rapid, error-free means of transferring data to provide a reasonable cycle of analyses and feedback. A problem that must be addressed is how to validate the accuracy and completeness of the automated output. The problem becomes more complex when the products generated through automated means also provide the information necessary for logistics support planning, for the preparation of technical manuals, the defining and optimization of spares procurement and placement, the technical requirements for test and other support equipment, the test procedures, the built-in-test routines, and all the data necessary for the LSAR.

Increasing reliance on computer systems for decision support is characteristic of both industry and DoD operations. As a result, legal standards of liability and risk must be applied in settings characterized by new methods of decision making and control. Data analysis may occur entirely in the computer, guided by analytical software, or may involve human judgment by a person who has little involvement with data entry. Both data and software errors can be difficult to correct even after discovery. An error in a single fact or computation can alter an entire analysis. Thus the integrity of data takes on great significance and incorrect data may be cause for unintended accidents, unnecessary design changes, and legal action.

The care used in the selection, maintenance, administration, and reliance on the system is at issue. Data inaccuracies resulting from poorly constructed and

monitored data entry systems are chargeable to those who control the systems. A failure to adopt data verification procedures constitutes a lack of reasonable care. While inaccurate data may arise even with reasonable care and without the knowledge of the relying users, knowingly selecting or relying on a system that either produces recurrent errors or is unable to perform a required function may be unreasonable and an independent basis for liability.

The risk of damage from lost or inaccurate data increases with the number of parties and the number of transactions. Even if only a few seconds elapse between the time of data communications until the time of data processing, the possibility of loss or damage must be taken into account especially since no hard copy of the data might exist. Furthermore, it might be difficult to track down the routes taken by the data; identify the operator processing them; and determine the time that the loss, mistake, or theft occurred.

When several discrete entities are involved in a complex system, it may be difficult to establish which one is responsible for a particular malfunction (e.g., data lost, forwarded to the wrong user, stolen, etc.). If only one entity operates the system, allocation of responsibility for error is less difficult. In some cases, on-line, real-time capabilities will result in constantly changing databases. Improved timeliness, increased quantity, and better quality of information produces higher quality, better-informed decisions. However, as a database is modified, the decision result may be impossible to reconstruct and be irrevocably altered. We need audit trails to control and record results of the decision process based on information in a complex and dynamic database. We must determine how much information we have to capture to provide the needed integrity for the decision process.

4.3.2 Copyright and Use of Software on Networks

For most purposes, sufficient laws are in place to protect copyrighted software such as that needed in CALS operations. However, different software and software implementations will have different requirements for protection. In many cases, industry and DoD personnel are not aware of what constitutes unauthorized reproduction or copyright infringement. DoD must properly train its management and staff in the various types of required protection and in the use of technologies designed to protect copyrighted software.

One of the rights granted to a copyright owner under Section 106 of Title 17 U.S.C. is the exclusive right to reproduce and to authorize the reproduction of the copyrighted work. Multiple copies of a program reproduced at different workstations or on different processors, in a network or multiuser configuration, could constitute copyright infringement. Some hold that loading a computer program into random access memory (RAM) or other volatile memory does not constitute the creation of a copy because the "copy" created is merely transitory. However, a copy of a program in volatile memory usually is not of fleeting or momentary duration; rather, the copy resides in memory for hours or days until the power is turned off.

Software stored on a file server or other storage device in a LAN can normally be accessed and copied by any workstation on the network. Creating copies of a program by manually transferring and inserting a diskette is illegal; downloading software from a file server to one or more personal computers (PCs) linked via a LAN or through some other form of communications media is equally illegal. Since multiple LANs may be interconnected by means of gateways, the range of potential users in the latter case is virtually unlimited.

Use of a program on a network may, therefore, involve unauthorized reproduction of copies. However, equivalent use of a program on a multiuser configuration where dumb terminals have access to the program resident on a central processor may not.

Whereas license agreements formerly prohibited the use of the software on a network, many software licenses now authorize use on any computer within the licensee's installation. LAN use is often expressly authorized, granting a user the right to electronically copy and distribute software. Software protection is more complex in a LAN environment. Some agreements prohibit any copies from being made, while others permit a limited number of copies for archival or backup purposes.

The many potential implementations of software in the CALS network will require the emplacement of specific control procedures. Management needs to be cognizant of agreements and protection for each software package in the network. Duplication of workstation authorized software through use of the network must be prevented. LAN and site-specific software, in turn, must not be illegally duplicated throughout the network. With the advent of high-level security protocols,

management will have a tool to more readily accomplish this protection. In the meantime, however, management must develop appropriate media control and authorization techniques to prevent illegal reproduction of copyrighted software.

4.4 DEVELOPING SECURITY TECHNOLOGIES

Section 2 included a discussion of the network security-related protocols to be used in OSI implementations. This section presents additional technology, either commercially available or under development, that may be appropriate for consideration by CALS programs; discusses network security and management standards; and describes management's role in security.

Examples of the types of promising network security technology currently being examined at NIST include

- *Random password generation devices.* With this device, a user can provide an authentication password that changes with every use. The device can be used with large- or small-scale systems and in data communications systems. A number of products, commonly known as "authentication calculators," are currently available.

- *Public-key encryption.* This will allow any two users to communicate securely across a network through the centralized distribution of encryption keys.

- *Communication port protection devices.* These devices protect the incoming communications line or port to a computer system. Typically, they answer the incoming call from a user, determine the user's claimed identity, and then hang up and call back to a predetermined telephone number. That procedure prevents a person from connecting to the network from an unauthorized location. It may limit, however, the flexibility of some users.

- *"Smart" card or key devices.* These devices are currently being tested at the NIST Institute for Computer Sciences and Technology (ICST) and are discussed below.

- *Trusted system engineering techniques.* NSA's NCSC is leading efforts to encourage the development of such systems engineering technology to bring down the cost of systems through wider availability. Currently, seven products are on the NSA Evaluated Products List.

- *Cryptography.* Cryptography is useful whenever information passes through "insecure channels." The physical accessibility of PCs and storage media make them insecure channels. The Data Encryption Standard (DES) is part of a standard on Computer Data Authentication.

A test lab at the NIST ICST is investigating smart cards and their use as access controls for networks. The smart card device includes a fingerprint reader, which sets off an alarm if an unauthorized user tries to sign on; it then prints the intruder's digitized fingerprint and displays the date, time, and identity of the cardholder whose card and password were fraudulently inserted. Biometric devices can identify fingerprints, hand geometry, palm prints, retina patterns, signatures, and voices. Costs range from $5,000 to $50,000.

Another security product related to the smart card is the smart key. The password is encrypted under DES by a $300 board inside the PC used as a terminal to the host computer. That encryption value is then stored in the key. The host computer decrypts the password and sends back a message to the key reader. The user cannot replay an earlier sign-on because the encryption value changes each time.

Access control devices developed by Time and Data Systems International (TDSI) include a "label and gateway" approach to security that ensures every object in the system from computer terminal to printer has a security "label" to determine whether it can pass through gateways to connect to other parts of the system. This technology is being implemented on the British Government's Central Computer and Telecommunications Agency (CCTA)systems.

Some manufacturers have introduced integrated systems with advanced network management features – audit trails, central site monitoring, and access control. An integrated system such as Avant Garde's Net/Guard can provide some of the more sophisticated capabilities, such as connecting authorized users to the network and appropriate host applications; controlling access through dial-back, user profiles, passwords and identification (user IDs), and logical access to applications; providing billboard and banner messages that enable the Network Control Center to communicate with dial-in users; providing real-time information on network status and alerting operators so corrective action can be taken in a timely manner; and providing audit trails that show the availability, use of resources, and activity of users.

4.4.1 Network Security and Management Standards

While there are many national and international protocol standards for network information interchange, there are no explicit network security or network

management standards. Standards can help achieve more secure systems that process correct data and allow only authorized persons access to data and systems. Standards will be needed for logging and analyzing security-significant events, for personal identification and access control methods, and for secure communications in networks.

The work to achieve standards for OSI will make it possible for different manufacturers' equipment to be interconnected through networks. Security standards will be an essential requirement for OSI networks as compatibility and interoperability objectives are achieved. The CALS telecommunications architecture provides additional information on standards and security.

4.4.2 Management's Role in Security

In the first annual report from NTISSC, the working group that was established by the President's National Security Decision Directive (NSDD)-145 describes the Government's posture in information systems security as "poor and rapidly getting worse," and in communications security as "unsatisfactory." The report recommends, in part, that the Government develop a coherent framework for computer security policies, and that such policies require each system that processes classified or sensitive data to have a personal identification and authentication system, audit trails that keep a record of activity, a designated security officer, a written security plan, control over physical access, and security controls on removable storage media. The report also calls for Cabinet-level action to increase manpower and funding in computer and communications security Government-wide. Cost-effective technical and management controls should be addressed in the early stages of system design and facilities management.

Many computer professionals believe that computer systems are often irresponsibly left unprotected because simple precautions are not taken. Such simple precautions include, for example, requiring the authority of two persons for disbursements, maintaining logs of system activity and scanning them for unusual patterns, changing standard passwords that are set for every system when they are first turned on, or using "dial-back" modems that require users to be at their authorized terminal locations.

While encryption has become more and more popular, only 6.5 percent of the agencies surveyed by OTA use encryption. Encryption does not provide total

protection, regardless of the strength of the encryption algorithm. Such an algorithm can prevent eavesdroppers from obtaining information through wiretapping activities but cannot prevent a person from logging into a system by using another user's account identification and password.

The opportunity to commit a computer crime is likely to increase as employees' computer skills increase. Placing too much responsibility in the hands of one person increases the risk. An ongoing risk management program should include periodic facility risk assessments and application reviews and audits to minimize the damage caused by fraud or the misuse of the computer systems. Auditing techniques for complex computer and communications systems are still evolving with the technology. Some staff members should be sufficiently trained to identify the risks and recommend and implement effective safeguards. A risk analysis can be quite lengthy and include a great deal of personal judgment. Simpler and less quantitative techniques for risk analysis are becoming more popular, especially for smaller information systems.

Managers and supervisors should have full knowledge of how systems under their control are being used and should implement and enforce security rules, making clear the consequences of their breach. When subordinates have access to Government information, whether classified or unclassified, managers have to anticipate the possibility of abuse, including sabotage and espionage. They have to ensure the proper precautions are taken and standards are established and followed.

GLOSSARY

ACSE	=	Associative Control Service Elements
ADP	=	automatic data processing
ANSI	=	American National Standards Institute
ARPANET	=	Advanced Research Projects Agency Network
ASCII	=	American Standard Code for Information Interchange
ASN.1	=	Abstract Syntax Notation
AUTODIN	=	Automatic Digital Network
B	=	Bearer
BAS	=	Basic Activity Subset
BCS	=	Basic Combined Subset
BOC	=	Bell Operating Company
BSS	=	Basic Synchronized Subset
CAD	=	computer-aided design
CAE	=	computer-aided engineering
CAI	=	computer-aided instruction
CAIS	=	Common Ada Interface Set
CALS	=	Computer-aided Acquisition and Logistic Support
CAM	=	computer-aided manufacturing
CASE	=	Common Application Service Elements
CCA	=	Computer Corporation of America
CCEP	=	Commercial COMSEC [Communications Security] Endorsement Program
CCITT	=	Consultative Committee on International Telephony and Telegraphy

CCL	=	common command language
CCR	=	commitment, concurrence, and recovery
CCTA	=	Central Computer and Telecommunications Agency (British)
CGM	=	Computer Graphics Metafile
CLID	=	calling line identification
CLNS	=	Connectionless Network Service
CMIP	=	Common Management Information Protocol
COMSEC	=	communications security
CONIT	=	Connector for Networked Information Transfer
COS	=	Corporation for Open Systems
CPE	=	customer premises equipment
CSIN	=	Chemical Substances Information Network
CSMA/CD	=	Carrier Sense Multiple Access with Collision Detection
CTN	=	CALS Test Network
D	=	Delta
DASS	=	Design Automation Standards Subcommittee
DBMS	=	database management system
DCA	=	Defense Communications Agency
DCE	=	data communications equipment
DCTN	=	Defense Commercial Telecommunications Network
DDF	=	Descriptive Data File
DDN	=	Defense Data Network
DES	=	Data Encryption Standard
DLA	=	Defense Logistics Agency
DLANET	=	DLA Network
DS0	=	Digital Signal Level 0; telephone term for a 64 Kilobit standard digital telecommunications channel

DTE	=	data terminating equipment
EBCDIC	=	Extended Binary Coded Decimal Interchange Code
EDI	=	Electronic Data Interchange
EDIF	=	EDI Format
EDMICS	=	Engineering Drawing Management Information and Control System
EIA	=	Electronic Industries Association
EIM	=	Engineering Information Model
EIS	=	Executive Information System
ES-to-IS	=	end-system-to-intermediate-system
FAR	=	Federal Acquisition Regulation
FED-STD	=	Federal Standard
FIPS	=	Federal Information Processing Standard
FRED	=	Front End for Databases
FTAM	=	File Transfer Access and Management
FTP	=	File Transfer Protocol
FTS	=	Federal Telecommunications System
FY	=	fiscal year
GKS	=	Graphical Kernel Standard
GML	=	Generalized Markup Language
GOSIP	=	Government Open Systems Interconnection Profile
GTE	=	General Telephone and Electronics Laboratories, Inc.
H	=	higher speed
HDLC	=	High-level Data Link Control
ICAM	=	Integrated Computer-Assisted Manufacturing
ICST	=	Institute for Computer Sciences and Technology
IDA	=	Intelligent Database Assistant

IDEF	=	ICAM Definition
IDS	=	Integrated Design Support
IEEE	=	Institute of Electrical and Electronic Engineers
IG	=	intelligent gateway
IGES	=	Initial Graphics Exchange Specification
IMP	=	Interface Message Processor
INGRES	=	Interactive Graphics and Retrieval System
INRIA	=	Institut National de Recherche en Informatique et en Automatique
IP	=	Internet Protocol
IPAD	=	Integrated Programs for Aerospace-Vehicle Design
IPMS	=	Interpersonal Messaging Service
IS-to-IS	=	intermediate-system-to-intermediate-system
ISDN	=	Integrated Services Digital Network
ISO	=	International Standards Organization
Kbps	=	Kilobits per second
LAN	=	local area network
LAP-B	=	Link Access Procedure-Balanced
LAP-D	=	Link Access Procedure-Delta
LLC 1	=	Logical Link Control Class 1
LLNL	=	Lawrence Livermore National Laboratory
LMI	=	Logistics Management Institute
LSAR	=	logistics support analysis record
MAC	=	media access control
MAP	=	Manufacturing Automation Protocol
Mb	=	Megabit
Mbps	=	Megabits per second
MCC	=	Microelectronics and Computer Technology Corporation

MHS	=	Message Handling System
MILNET	=	Military Network
MIL-STD	=	Military Standard
MIT	=	Massachusetts Institute of Technology
MIU	=	Media Interface Unit
MODELS	=	Modernization of Defense Logistics Standard Systems
MRDSM	=	MULTICS Relational Data Store Multidatabase
MTS	=	Message Transfer Service
NASA	=	National Aeronautics and Space Administration
NCSC	=	National Computer Security Center
NDL	=	Network Data Language
NFAIS	=	National Federation of Abstracting and Information Services
NIST	=	National Institute of Standards and Technology
NLM	=	National Library of Medicine
NSA	=	National Security Agency
NSDD	=	National Security Decision Directive
NTISSC	=	National Telecommunications and Information Systems Security Committee
O&M	=	operation and maintenance
OMB	=	Office of Management and Budget
OSI	=	Open Systems Interconnection
OSINET	=	OSI Network
OTA	=	Office of Technology Assessment
PC	=	personal computer
PDDI	=	Product Data Definition Interface
PDES	=	Product Definition Exchange Specification
PDN	=	Public Data Network

PHIGS	=	Programmer's Hierarchical Interactive Graphics Standard
P.L.	=	Public Law
PLP	=	Packet-Level Protocol
PSN	=	packet-switching node
RAM	=	random access memory
RDAP	=	Remote Data Access Protocol
RF	=	radio frequency
R&D	=	research and development
R&M	=	reliability and maintainability
SASE	=	Specific Application Service Elements
SDC	=	Systems Development Corporation
SDNS	=	Secure Data Network System
SGML	=	Standard Generalized Markup Language
SMTP	=	Simple Mail Transfer Protocol
SNA	=	Systems and Network Architecture Division
SNACF	=	Subnetwork Access Convergence Facility
SNDCP	=	Subnetwork Dependent Convergence Protocol
SPAWAR	=	Space and Naval Warfare Systems Command
SQL	=	Structured Query Language
SUNY	=	State University of New York
T1	=	1.544 Mbps Standard used in the United States
TAC	=	Terminal Access Controller
TCP	=	Transmission Control Protocol
TCSEC	=	Trusted Computer Security Evaluation Criteria
TDSI	=	Time and Data Systems International
Telenet	=	Telecommunications Network
TIS	=	Technical Information System

TNI	=	Trusted Network Interpretation
TOP	=	Technical Office Protocol
TP-0	=	Transport Protocol Class 0
TP-4	=	Transport Protocol Class 4
Tynmet	=	Tymshare Corporation Network
UDI	=	unrestricted digital information
UIMS	=	User Interface Management Service
U.S.C.	=	United States Code
VHDL	=	VHSIC Hierarchical Definition Language
VHSIC	=	Very High Speed Integrated Circuit
VTP	=	Virtual Terminal Protocol
WAN	=	wide-area network
WATS	=	Wide Area Telecommunications Service
WGIM	=	Working Group on Information Modeling

APPENDIX A

CALS DATA COMMUNICATIONS GUIDELINE

CONTENTS

		Page
1.0	Near-Term Communications (1989 – 1990)	A- 3
1.1	Lower-Layer Communications	A- 4
1.2	Upper-Layer Protocols	A-11
1.3	Internetworking	A-16
1.4	Security Implications	A-25
1.5	Vendor-Provided Capabilities	A-26
1.6	Industry Interfaces	A-27
1.7	Summary of Near-Term CALS Communications	A-27
1.8	Transition to Mid-Term Objectives	A-29
2.0	Mid-Term Communications (1991 – 1992)	A-29
2.1	Protocol Additions/Enhancements	A-29
2.2	Internetworking	A-33
2.3	Security Implications	A-35
2.4	Summary of Mid-Term Communications	A-36
2.5	Transition to Long-Term Objectives	A-36
3.0	Long-Term Communications (1993 – 1994)	A-38
3.1	Additional/Enhanced Protocols	A-38
3.2	Long-Haul Environment	A-39
3.3	Security Implications	A-43

CALS DATA COMMUNICATIONS GUIDELINE

The Computer-aided Acquisition and Logistic Support (CALS) telecommunications architecture, or data communications guideline, provides a comprehensive list of data communications protocols, data exchange protocols, and transmission media to be used to facilitate communications among the Services and industry contractors. This guideline is divided into three chronological sections or phases serving as a timetable for implementing functions and protocols on the basis of the anticipated availability of the required technologies. The protocols and capabilities outlined in each phase are to be implemented by the end of the specified period.

The near-term phase, covering 1989 – 1990, concentrates on commercially available, off-the-shelf technology or software that, realistically, can be developed and implemented in this period. During the near-term phase, limited use of the Defense Data Network (DDN) is expected. The mid-term phase concentrates on technology that will become stabilized/standardized in 1991 – 1992. The ability of the DDN to support all the required protocols will probably become available during the mid term. Additional capabilities will be offered by Federal Telecommunications System (FTS)-2000 in this period. The long-term phase, from 1993 – 1994, completes the communications architecture required to support the CALS environment and its specific needs. This phase should begin to provide the higher bandwidth services required to accommodate on-line transmission of increased volumes of CALS data.

The description of each phase builds upon that of the preceding phase in capabilities provided and contains recommendations on technology refreshment. Recommendations for transitioning to the next phase are provided at the end of the near-term and mid-term descriptions.

1.0 NEAR-TERM COMMUNICATIONS (1989 – 1990)

This section emphasizes commercially available technology and products that it is realistic to believe can be developed and implemented in the near term to support CALS projects. It is the intent of the near-term plan to concentrate on areas that will achieve the highest productivity gains. The protocols recommended are expected to be available within the near term, but may not be fully implemented by individual

be available within the near term, but may not be fully implemented by individual vendors at the beginning of the near-term phase. It is hoped that their inclusion as stated requirements will cause them to become more widely implemented and available from all vendors who wish to do business with DoD. Project managers should allow vendor solutions to be put into place until the required protocol support is made available. However, vendors should be required to comply with these specified protocols and implementations by the end of the near-term time frame.

Special attention is given to the local-area environment in this time frame, because the bulk of data transfer over geographically dispersed areas will generally be accomplished off line. In the near term, off-line media in the form of optical disks, magnetic media, hard copy, etc., will be the most cost-effective methods for distributing the large volumes of CALS data. The mechanisms that will be used to transfer the data are the Postal Service, express services, etc. Standard data exchange protocols and procedures should be followed when using off-line methods of communication.

1.1 Lower-Layer Communications

The lower-layer protocols – Physical, Data Link, and Network – in both the local-area environment and the long-haul environment are presented here. Hardware items are discussed where appropriate.

1.1.1 Local-Area Environment

This section describes the functional local area network (LAN) to support CALS projects in the local environment. Basewide communications are beyond the scope of this plan. The CALS project manager should investigate the ability of any installed or planned basewide LAN to accommodate transmission and connectivity requirements of CALS projects. If an existing LAN is capable of meeting specific CALS project requirements, it should be used. If not, selection of a functional local communications medium depends on many variables. The following is provided to help project managers decide which type of technology to employ to meet specific requirements:

- The number of end and intermediate systems required to be connected
- The physical area to be served by these systems and the maximum distance between the most remote end systems

- Possible future expansion, both in number of connections and in distance
- Ease of installation
- Performance in terms of transmission rate and maximum packet length
- Reliability
- Security considerations
- Immunity from electrical interference
- Compliance with international standards and Government Open Systems Interconnection Profile (GOSIP) implementation specifications
- Availability of compatible components from more than one supplier
- Ease of maintenance
- Ability to communicate outside the LAN through gateways to DDN and to other base/campus LANs
- Cost in relation to performance.

1.1.1.1 Physical Layer. Two options are specified for media at the Physical Layer for use in the local environment: broadband bus or baseband bus. The choice of physical medium depends on the individual project and its particular goals. A brief description of both types of media is given to help the project manager determine the most suitable alternative.

The bandwidth provided by a broadband bus is similar to that of cable television, which can simultaneously handle dozens of different television signals. This type of medium uses frequency division multiplexing to divide the total bandwidth [approximately 400 Megabits per second (Mbps)] into separate channels to accommodate various types of traffic. This traffic can be in the form of data, voice, or image. To accomplish this simultaneous communications operation, all stations must use either a frequency-agile or fixed-frequency type of radio frequency (RF) modem to gain access to the physical medium. Among broadband's strengths are its ability to transmit various types of information (e.g., video, data, voice) over the same medium at the same time, ease of reconfiguration, and suitability for campus-sized LANs spanning several miles. A 10Broad36 broadband network may extend 3,750 meters (1,875 meters from the head-end location). Cabling consists of 75-ohm coaxial cable.

A baseband bus is used to transmit primarily data traffic; it provides only one transmission channel at a time. Baseband media typically provide a data rate of 10 Mbps, limited to 500-meter network segments (this distance may be extended to 2,800 meters by using baseband repeaters) and a maximum of 1,025 nodes. A repeater is a transparent device used to connect segments of an extended network at the Physical Layer. Only networks of one type may be interconnected using this method (i.e., physical layers must be identical). Cabling consists of 50-ohm coaxial cable. This type of medium is often favored for the office environment, which generally does not require the additional capacity and expense to handle multiple channels.

The costs associated with broadband and baseband media are directly related to the bandwidth that each provides. In general, the broadband method is about twice as expensive as its baseband counterpart, because of requirements for RF modems, head-end remodulator, and physical cable plant. Maintenance costs associated with the two media and the related issue of maintenance staff requirements must also be considered. Maintenance of broadband networks is more difficult and expensive, because placement, replacement, and tuning of their active components to service or expand the network requires the skill of highly trained technicians. Baseband, being a passive network technology, does not require the same degree of technical support and is, therefore, less expensive to maintain.

On the basis of the foregoing, it is recommended that the baseband (10Base5) standard become the primary standard for CALS projects, since there is generally no need to support multiple types of traffic (e.g., voice) and because of the costs associated with broadband. If there is a compelling reason for using broadband (e.g., more than one 10 Mbps data channel is required to support the LAN traffic load), then Broadband (10Broad36) should be specified, allowing several data channels to operate over the same cable. Appendix B, Network Capacity Planning, provides guidance to help the project manager determine the transmission media based on projected traffic volumes.

1.1.1.2 Media Access Control. The media access control (MAC) function, applicable to LANs, can be considered a sublayer of the International Standards Organization (ISO) Data Link Layer. MAC selection depends on the particular

environment. The acquisition authority must choose from the following types of MAC:

- Institute of Electrical and Electronic Engineers (IEEE) 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC
- IEEE 802.4 Token Bus MAC.

Media access control specifies how the individual stations on the physical network gain access to the backbone medium. In the IEEE 802.4 token-passing method, permission to use the network is passed from station to station in a predetermined order. This protocol is deterministic, guaranteeing access to the network by every station within a predictable period. This deterministic access capability is very important in the factory environment or other similar environments where critical data regarding the status of a factory robotic device might need to be reported to a control program in an absolutely predictable manner.

The CSMA/CD MAC is a contention access method in which each station on the bus contends for the physical medium. Access to the network by a specific station cannot be guaranteed within a certain time period. With the CSMA/CD access scheme, a station desiring to transmit data listens to the medium to determine whether it is in use. If it is, the station does not transmit. If the medium is not being used, the station transmits its data and monitors the medium to detect a collision of its data with data from another station. If a collision is detected, the station backs off for a preset time and then attempts retransmission.

Comparing the two types of media access methods, token-passing and CSMA/CD, assists the project manager in determining the most appropriate technology. Traffic load characteristics heavily influence the selection of a particular media access technique.

Generally, deterministic protocols are better suited for heavy traffic loads than the contention-based probabilistic protocols because they allocate the available bandwidth more efficiently by giving each station a predetermined access to the medium. When traffic loads are light, however, deterministic protocols provide individual stations with slower response and less throughput in comparison with contention-based probabilistic protocols. The slower response results from stations having to wait their turn even though no other station may have anything to

transmit. The smaller throughput results from limitations on the amount of data a station can send before it has to relinquish access to the medium.

Probabilistic protocols have the opposite traffic-handling characteristics. They behave poorly under heavy traffic loads because transmission bandwidth is wasted by stations contending for the medium, resulting in an increase in the number of collisions that occur. But under light traffic loads, they provide stations with quicker response and higher throughput than deterministic protocols. Quicker response is possible because stations can immediately access the medium whenever it is idle. Higher throughput results from the ability to access the medium quickly and repeatedly without the delay inherent in a token-passing deterministic scheme. Probabilistic access methods are more suited for bursts of random, unpredictable traffic common in the office environment. There is currently much debate in the industry regarding traffic load that would cause the probabilistic media access method to degrade in performance. Generally, it is agreed that degradation occurs when between 60 and 90 percent of the capacity is utilized.

On the basis of the preceding discussion, it is recommended that the IEEE 802.3 CSMA/CD MAC be specified for CALS projects. CSMA/CD is better suited to CALS traffic requirements, and it allows for easy migration from an existing installed base of Ethernet LANs. These LANs have been installed by several CALS prototype projects, and there is wide availability of network components that have been developed for Ethernet networks. Also, the CSMA/CD technology running on the 10 Mbps cable has proven capable of handling a variety of technical and office applications, from document interchange to graphics interchange, both business and engineering. If several data channels are required to accommodate the traffic load and broadband is selected, then each channel should use CSMA/CD media access methodology.

1.1.1.3 Media Interface Units. Media Interface Units (MIUs) are physical entities that must be specified for each type of engineering workstation, display terminal, peripheral device (e.g., shared printers and optical scanners), host processor, and intermediate internetworking system to be connected to the LAN. The concept of MIUs may not apply if intelligent boards are developed and available. The MIU serves as a node to connect distributed processing devices either directly or indirectly to the network. MIUs provide communications without requiring a central network processor. Every piece of DTE requiring connection to the LAN will require

an MIU to provide the electrical and logical interface between the DTE and the network, to control transmissions into the network, and to act upon data received from the network. The MIU should provide a DTE physical interface and operate with the specific DTE Protocols. MIUs should be available for both asynchronous and synchronous DTEs and support a variety of transmission speeds.

1.1.1.4 Data Link Layer. The Data Link Layer Protocol specified for use in the local environment is the IEEE 802.2 Logical Link Control Class 1 (LLC 1). This protocol provides a communications service that allows for the exchange of data between two logical entities without the establishment of a connection (connectionless-oriented communication). Message sequencing, acknowledgment, flow control, and error recovery functions are provided by the upper layers. The RS-232 [Electronic Industries Association (EIA) standard interface between data terminating equipment (DTE) and data communications equipment employing serial binary data interchange] is used for low volume requirements at data rates up to 9.6 Kilobits per second (Kbps). Larger data volumes will operate at 56 Kbps using V.35 standards [Consultative Committee on International Telephony and Telegraphy (CCITT) standard governing data transmission at 48 – 64 Kbps].

1.1.1.5 Network Layer. The following ISO Network Layer standards are to be implemented by CALS projects in end systems and intermediate systems, in accordance with the National Institute of Standards and Technology (NIST) workshop agreements and the GOSIP baseline:

- ISO Connectionless Network Service (CLNS)
  - ISO IS 8348 Network Service Definition
  - ISO IS 8348/AD1 Connectionless Data Transmission
  - ISO IS 8348/AD2 Network Layer Addressing
  - ISO DIS 8648 Internal Organization of the Network Layer
  - ISO IS 8473 Protocol for CLNS
  - ISO IS 8473/AD1 Provisioning of the Underlying Services.

1.1.2 Long-Haul Communications

The existing suite of DoD protocols will gradually transition to the Open Systems Interconnection (OSI) protocols. This transition, which will take several

years, will include a period in which both the DDN and OSI protocol suites will be supported. Both protocol suites have promoted the same lower-layer protocols to achieve connection to a wide-area network (WAN). Regardless of which upper-layer communications protocols are used, all CALS projects should specify an X.25 DTE-to-data communications equipment (DCE) interface with the appropriate Defense Communications Agency (DCA)/DoD specified options and parameters. The X.25 DTE-to-DCE defines the Network Access Protocol to be used to access DDN regardless of the upper-layer protocols selected. It is very important to inform DCA as soon as possible of circuit requirements, since a leadtime of 18 to 24 months is required to obtain a physical circuit. Information regarding anticipated needs can be sent to the Defense Communications Agency, Code B610, Washington, DC, 20305.

In many cases, either on a temporary basis or where exemptions have been granted, connectivity can be accomplished through commercial public data X.25 networks such as Data America/Bell Operating Companies, or Telenet, allowing for DDN-like capability. Such circuits might be implemented among vendors or among vendors and select Government entities on a specific project. This type of service offers short leadtimes (6 to 12 weeks) and may reduce costs.

1.1.2.1 Physical Layer. The physical interface speed required to support project requirements depends on traffic volumes. Two physical interface standards are presented. The CALS project manager should choose one physical interface standard or multiples of one, on the basis of projected data transmission requirements. The Physical Layer standard chosen should meet all the requirements of the DDN document, *X.25 Host Interface Specification*. Specifying multiple 56 Kbps subscriber access links using the same single 56 Kbps backbone trunk merely moves the bottleneck to the connecting packet-switching node (PSN).

- For projects with low-volume requirements (e.g., inquiry only), the interchange circuit(s) should operate at the data rate of 9.6 Kbps using the RS-232-C physical interface in accordance with Federal Information Processing Standard (FIPS) 100/Federal Standard (FED-STD) 1041.
- For projects having a large volume of data to transfer (i.e., bulk transfer), the interchange circuit should operate at the data rate of 56 Kbps in accordance with CCITT Standard V.35.

1.1.2.2 Data Link Layer. The Data Link Protocol specified is CCITT High-level Data Link Control (HDLC) Link Access Procedure Balanced (LAP-B), implementations of which must meet the requirements of DDN document *X.25 Host Interface Specification.* X.25 LAP-B is further defined by specifying FIPS 100/FED-STD 1041. The Multilink Sublayer should be specified where multiple physical links are required to accommodate greater traffic volumes.

1.1.2.3 Network Access Layer. The Network Access Protocol specified is the CCITT X.25 Presentation Level Protocol (PLP), implementations of which must meet the requirements of DDN document *X.25 Host Interface Specification.* X.25 at the Network Layer is further defined by specifying FIPS 100/FED-STD 1041.

Information regarding connection to the DDN can be obtained from the Defense Communications Agency, Code B610, Washington, DC, 20305.

1.1.2.4 Network Layer. The ISO Network Layer standards listed in Section 1.1.1.5 of this appendix are to be implemented by CALS projects for both end systems and intermediate systems, in accordance with the NIST workshop agreements and the GOSIP baseline.

1.2 Upper-Layer Protocols

All CALS procurements should specify the upper-layer protocols listed in this guideline rather than the standard DDN protocol suite [File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and TELNET] or any proprietary vendor-unique protocols. DoD protocols or vendor-unique solutions may be used until the required protocols can be developed and implemented. Use of the present DoD Transmission Control Protocol/Internet Protocol (TCP/IP) is recommended to provide interoperability until the CALS-specified protocols can be developed and implemented. However, no new developments of the current DDN protocol suite should be funded by CALS project procurements.

The protocols specified by this guideline are to be in place by the end of 1990. The CALS protocols will continue to be based on the NIST OSI Implementors Workshop Agreements and will come in the form of a specification developed from the GOSIP baseline. Since the GOSIP document and the workshop agreements will be modified in the future, project managers and vendors must ensure the appropriate version is being reviewed.

The protocols specified in this section establish the baseline architecture for providing connectivity between end systems in the CALS environment. End systems are considered to be "peer" systems; that is, an end system is capable of communicating with any other end system by implementing the following protocols, regardless of the underlying lower-layer protocols implemented to support physical connectivity.

1.2.1 Transport Layer

The common transport protocol, ISO Transport Protocol Class 4 (TP-4), is a connection-oriented protocol. TP-4 provides multiplexing, error detection, and error recovery to the transport user. Specifically, TP-4 service ensures data are not lost, duplicated, or corrupted in transit and that they arrive at their destination in the right order. TP-4 has end-system-to-end-system significance, where each end is defined as a corresponding transport entity. ISO Transport Protocol Class 0 (TP-0) is to be used with connection-oriented Public Data Network (PDN) messaging only. The following ISO Transport Layer standards are to be implemented by CALS projects, in accordance with the NIST workshop agreements and the GOSIP baseline:

- ISO TP-4
  - ISO IS 8072 Transport Service Definition
  - ISO IS 8073 Transport Protocol Specification
  - NIST Institute for Computer Sciences and Technology/Systems and Network Architecture Division (ICST/SNA)-85-17 Military Supplement
  - NIST ICST/SNA-85-18 Implementors Guide
- ISO TP-0 (needed only to access PDN X.400 message systems).

1.2.2 Session Layer

The common session protocol, ISO Session, provides a means for cooperating presentation entities to organize and synchronize their conversation and to manage data exchange. The ISO has defined three subsets of the 12 functional units that make up the Full Session Protocol: the Basic Combined Subset (BCS), Basic Synchronized Subset (BSS), and Basic Activity Subset (BAS). Different subsets are required by different application protocols. The following ISO Session Layer

standards are to be implemented by CALS projects, in accordance with the NIST workshop agreements and the GOSIP baseline:

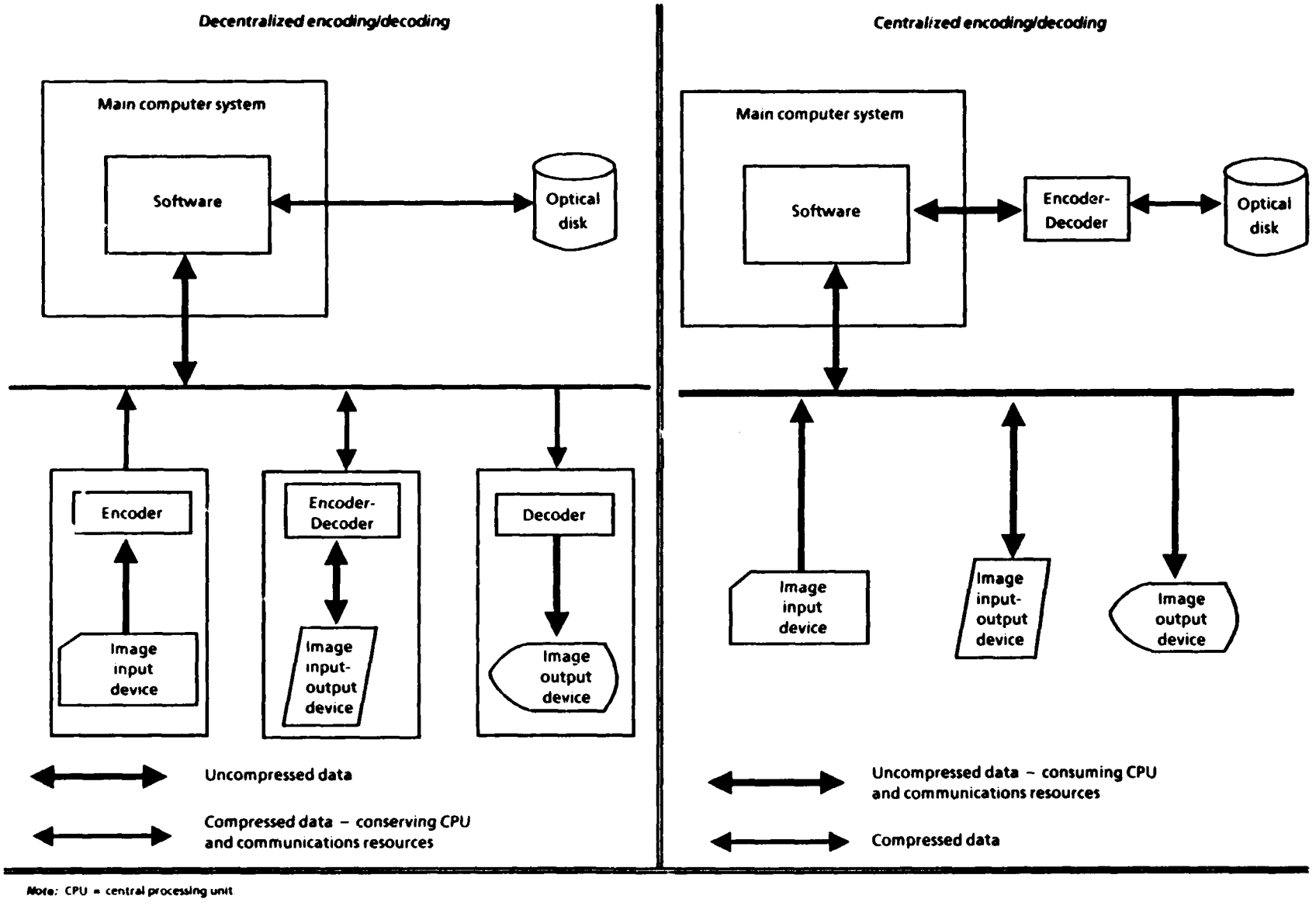
- ISO Session Services and Protocol
  - ISO IS 8326 Session Service Definition
  - ISO IS 8327 Session Protocol Specification.

1.2.3 Presentation Layer

The common presentation protocol, Abstract Syntax Notation (ASN.1), specifies rules for defining and recording the meaning, or semantic content, of messages. The following ISO Presentation Layer standards are to be implemented by CALS projects in accordance with the NIST workshop agreements and the GOSIP baseline:

- ISO Presentation Services and Protocol
  - ISO DIS 8822 Connection-Oriented Presentation Service Definition
  - ISO DIS 8823 Protocol Specification
  - ISO DIS 8824 Specification of ASN.1
  - ISO DIS 8825 Basic Encoding Rules for ASN.1.

All image data that will traverse the network should be in compressed format. A conservative estimate is a 10:1 compression ratio, with the present CCITT Group 4 standard implementations. New fractal compression technology may increase this ratio to 1,000:1. Compression/decompression units should be placed at the points of data origin and use. By compressing data at the input source (i.e., graphics modification terminal or aperture card scanner) and decompressing the output data at the target output device (i.e., plotter or graphics display terminal), the communications paths are relieved of the burden imposed by transmitting uncompressed image data. Compression units on the market today provide compression speeds of 20 Megapixels per second. Compression/decompression units are becoming readily available and can be found as board-level implementations. Figure A-1 graphically compares the decentralized and centralized approaches to encoding/decoding of image data.



Note: CPU = central processing unit

FIG. A-1. CALS IMAGE ENCODING/DECODING COMPARISON

1.2.4 Application Layer

The Associative Control Service Elements (ACSE) is an Application Service Element (ASE) just like File Transfer Access and Management (FTAM) and provides general-use capabilities to applications. Two application layer protocols will be provided to CALS projects in the near term: FTAM and the CCITT X.400 Message Handling System (MHS). The FTAM Protocol will provide the Reliable File Service level of service. The FTAM implementation will support binary, textual, and directory file types. FTAM is logically divided into two sections. The first section, File Transfer Protocol (FTP), deals primarily with the way a file is moved from one system to another. The second section, File Access and Management, deals with file attributes and protection. The CCITT X.400 MHS will support electronic mail. The following ISO Application Layer standards are to be implemented by CALS projects, in accordance with the NIST workshop agreements and the GOSIP baseline:

- ISO Common Application Service Elements (CASE)
  - ISO DIS 8649/1 General Introduction
  - ISO DIS 8649/2 ACSE
  - ISO DIS 8650/2 Protocol Specification for CASE
- ISO FTAM
  - ISO DIS 8571/1 General Introduction
  - ISO DIS 8571/2 Virtual Filestore
  - ISO DIS 8571/3 File Service Definition
  - ISO DIS 8571/4 File Protocol Specification
- CCITT X.400 MHS
  - CCITT X.400 Series Implementors Guide
  - CCITT X.400 System Model-Service Elements
  - CCITT X.[illegible]1 Basic Service Elements and Options
  - CCITT X.408 Encoded Type Conversion Rules
  - CCITT X.409 Presentation Transfer Syntax and Notation
  - CCITT X.410 Remote Operations and Reliable Transfer Service

- CCITT X.411 Message Transfer Service (MTS)
- CCITT X.420 Interpersonal Messaging Service (IPMS).

1.2.5 Protocol Applicability

All end systems (e.g., workstations, peripheral devices, servers, display terminals, host processors, etc.) connected to the LAN are to interoperate via the upper-layer protocols specified in the near-term phase. Figure A-2 is an architectural seven-layer model that depicts the near-term protocol suite for end systems connected to the CALS LAN. This suite contains the required lower- and upper-layer protocols.

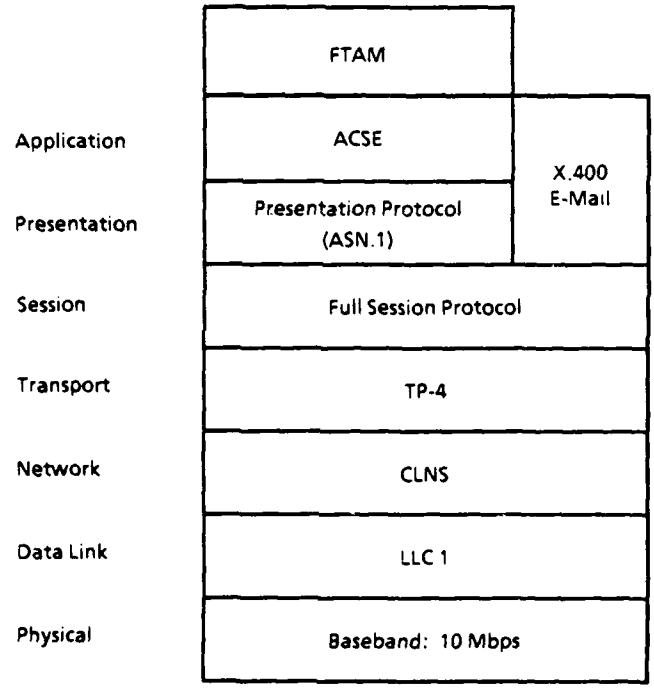


FIG. A-2. CALS NEAR-TERM PROTOCOLS (1989 – 1990) – END SYSTEMS

1.3 Internetworking

This section addresses the concerns associated with internetworking in both the local and long-haul environment.

1.3.1 Internetworking in the Local Environment

The ability of the existing base LAN to support transmission requirements of specific CALS projects should be investigated. Individual CALS projects must specify local requirements for internetworking the CALS LAN to other base or campus type LANs. The individual CALS projects should evaluate existing or planned basewide interconnection plans and specify additional interconnection/internetworking hardware and software as required. The exact configuration to use depends on the protocol stacks of LANs to be internetworked.

- *Identical protocol stacks.* Repeaters may be used to interconnect identical LANs using identical protocol stacks. Limitations in distance are imposed by the electrical properties of the media.

- *Protocol stacks identical above the Physical Layer.* A bridge may be used to support network expansion by connecting two physically distinct networks at the Data Link Layer. The two networks must use a consistent addressing scheme and frame size. Interconnection relies on the use of identical Data Link Protocols on connected networks. The base/campus LAN must use the LLC 1 Protocol at the Data Link Layer.

- *Protocol stacks identical above the Data Link Layer.* An intermediate system provides connectivity between physically distinct networks at the Network Layer. One of the major goals of this CALS telecommunications plan is to keep the Network Layer Protocol consistent across all the various subnetworks. The implementation of the ISO IP will make internetworking easier to administer, control, and manage. The various subnetwork types can have their services mapped to the ISO IP via a Subnetwork Dependent Convergence Protocol (SNDCP) and a Subnetwork Access Convergence Facility (SNACF). Figure A-3 depicts the interconnection of the CALS functional LAN and the base LAN, both of which use the ISO protocols.

- *Dissimilar protocol stacks.* If the base or campus LAN protocol stack is not of the ISO/GOSIP type, a full gateway must be implemented to accomplish interoperability. If the base LAN is built around the present suite of DoD protocols, the NIST application gateway may provide the internetworking function. Figure A-4 depicts this situation.

1.3.2 Internetworking in the Long-Haul Environment

The following discussion for internetworking in the long-haul environment is based on the use of the DDN as mandated by DoD.

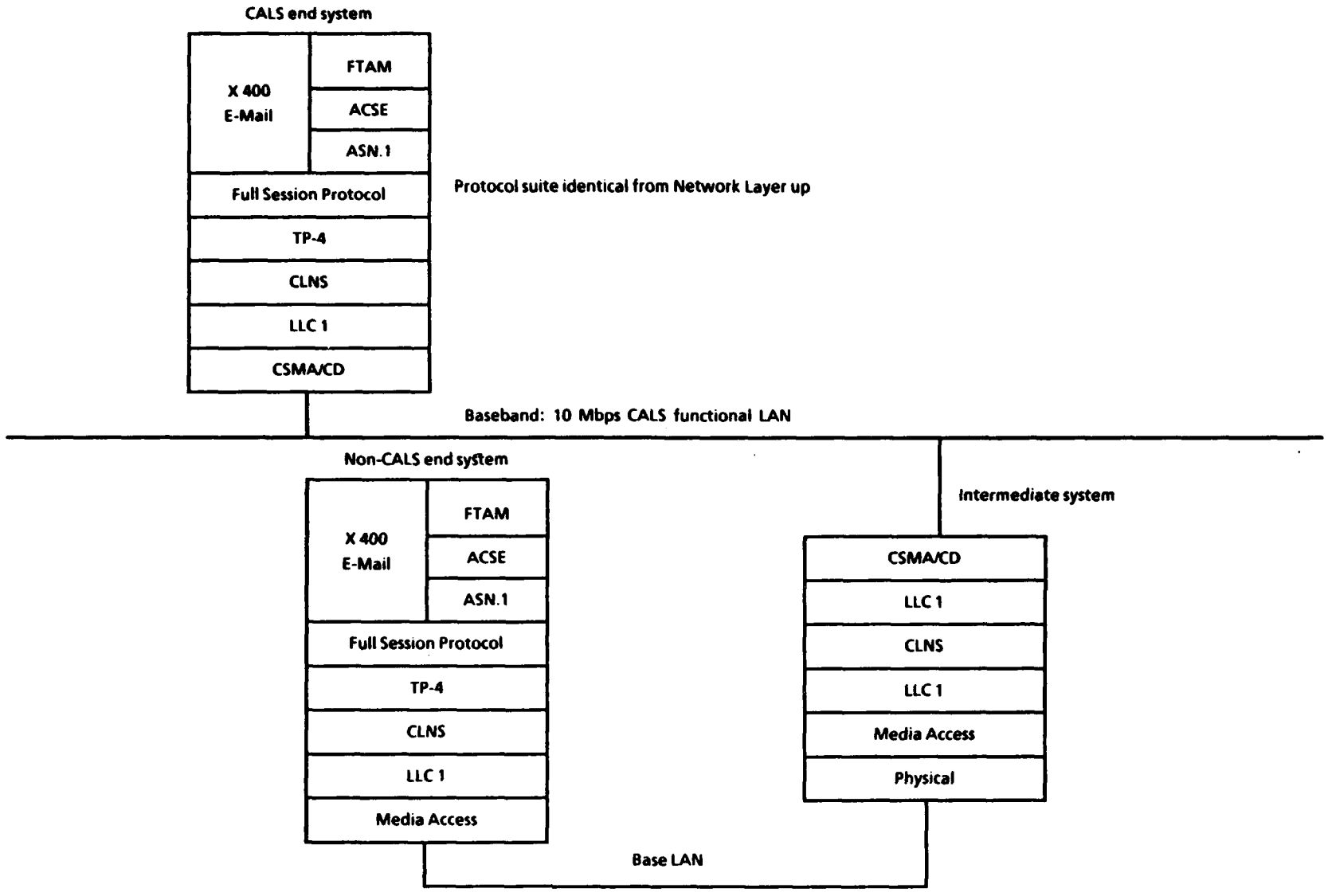
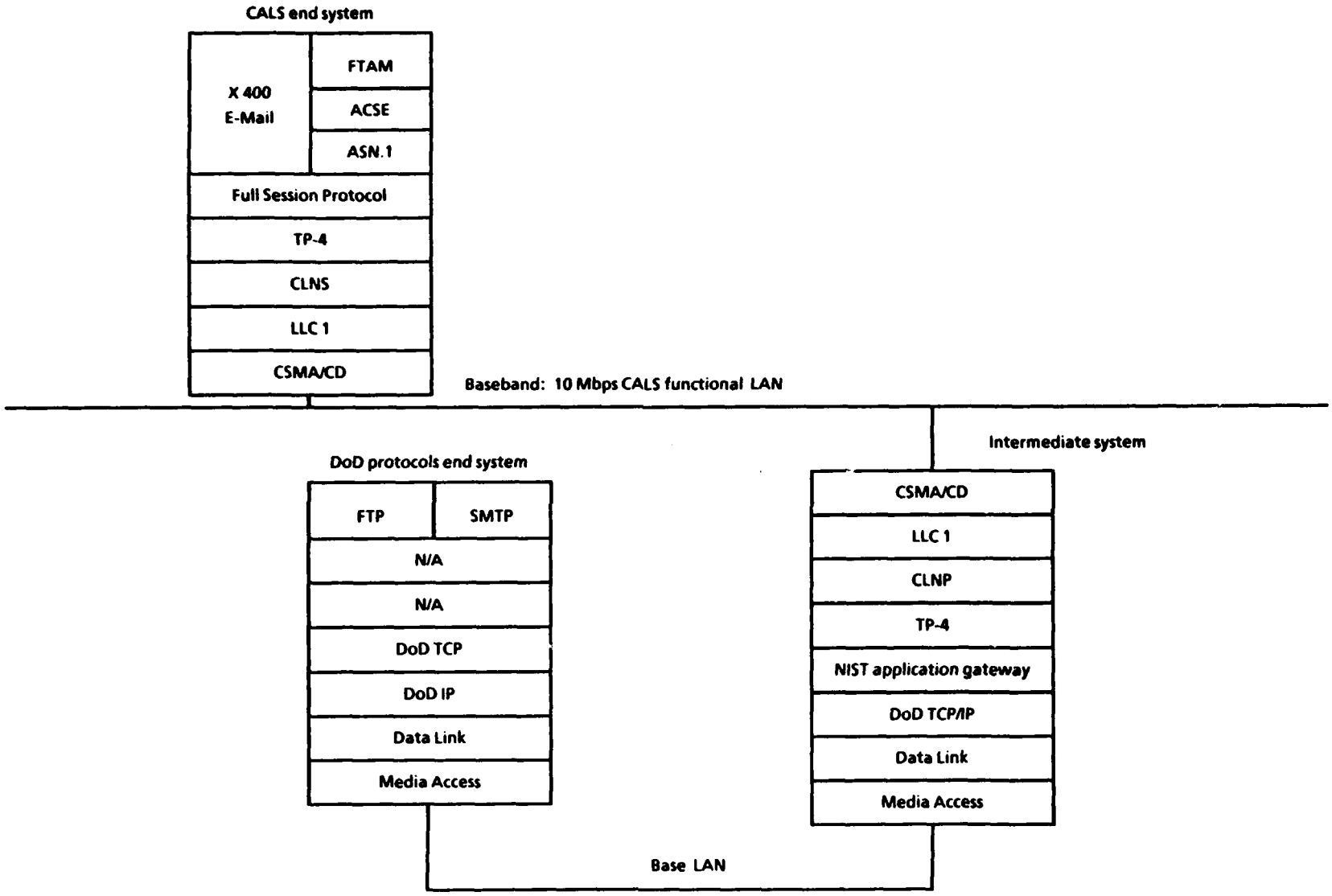


FIG. A-3. CALS LOCAL AREA NETWORK INTERCONNECTION WITH BASE BACKBONE GOSIP LOCAL AREA NETWORK



Note: N/A = not applicable

FIG. A-4. CALS FUNCTIONAL LOCAL AREA NETWORK INTERCONNECTION WITH BASE BACKBONE DoD LOCAL AREA NETWORK

1.3.2.1 Intermediate System for DDN Connectivity. DCA is developing a plan to support coexistence of the ISO protocols and the DDN protocol suite. Use of the DDN will be limited until the end-system-to-intermediate-system (ES-to-IS) protocol, intermediate-system-to-intermediate-system (IS-to-IS) protocol, and Virtual Terminal Protocol (VTP) are added to the GOSIP baseline. The absence of VTP will prevent use of the DDN Terminal Access Controller (TAC) and Mini-TAC in the near term. A further limitation is imposed by the 56 Kbps transmission rate on subscriber access links and backbone media. Until these protocols are included and the physical bandwidth is increased, the DDN should be used only for inquiry-type traffic, electronic mail applications, and high-priority/low-bandwidth file transfer traffic.

The intermediate system to support communications over an X.25 connection-oriented WAN between end systems implementing the near-term-specified ISO protocols is based on the use of CLNS and SNDCP. SNDCP specifies use of the underlying subnetwork protocol in order to work with CLNS. SNDCP will reside between the CLNS and the DDN-specified X.25 PLP on the internetworking unit. This intermediate system will provide a virtual circuit to another X.25 intermediate system. The destination X.25 gateway node will complete the circuit to the destination end system. The path consists of three separate virtual links; origin end system to origin X.25 gateway node, origin X.25 gateway node to destination X.25 gateway node, and destination X.25 gateway node to destination end system. Figure A-5 depicts an architectural model of the intermediate system required to support DDN connectivity. Figure A-6 depicts the architecture to support communications over DDN for the CALS closed community.

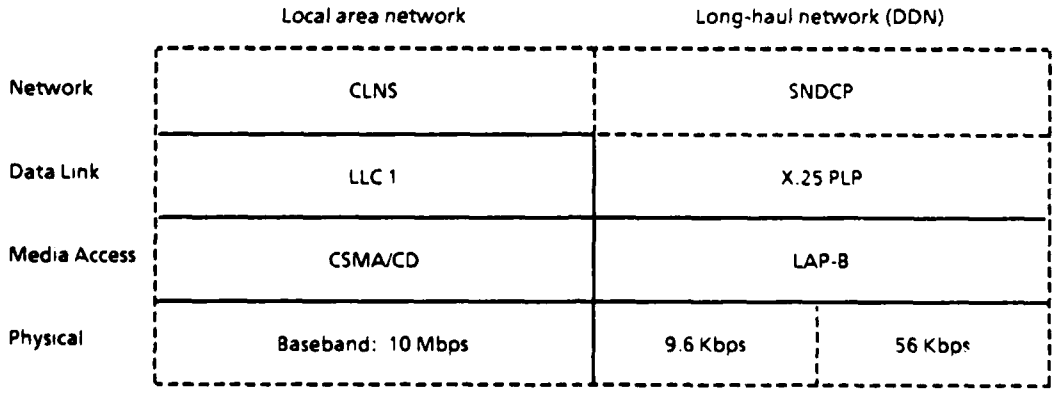


FIG. A-5. CALS NEAR-TERM PROTOCOLS (1989 – 1990) – INTERMEDIATE SYSTEM

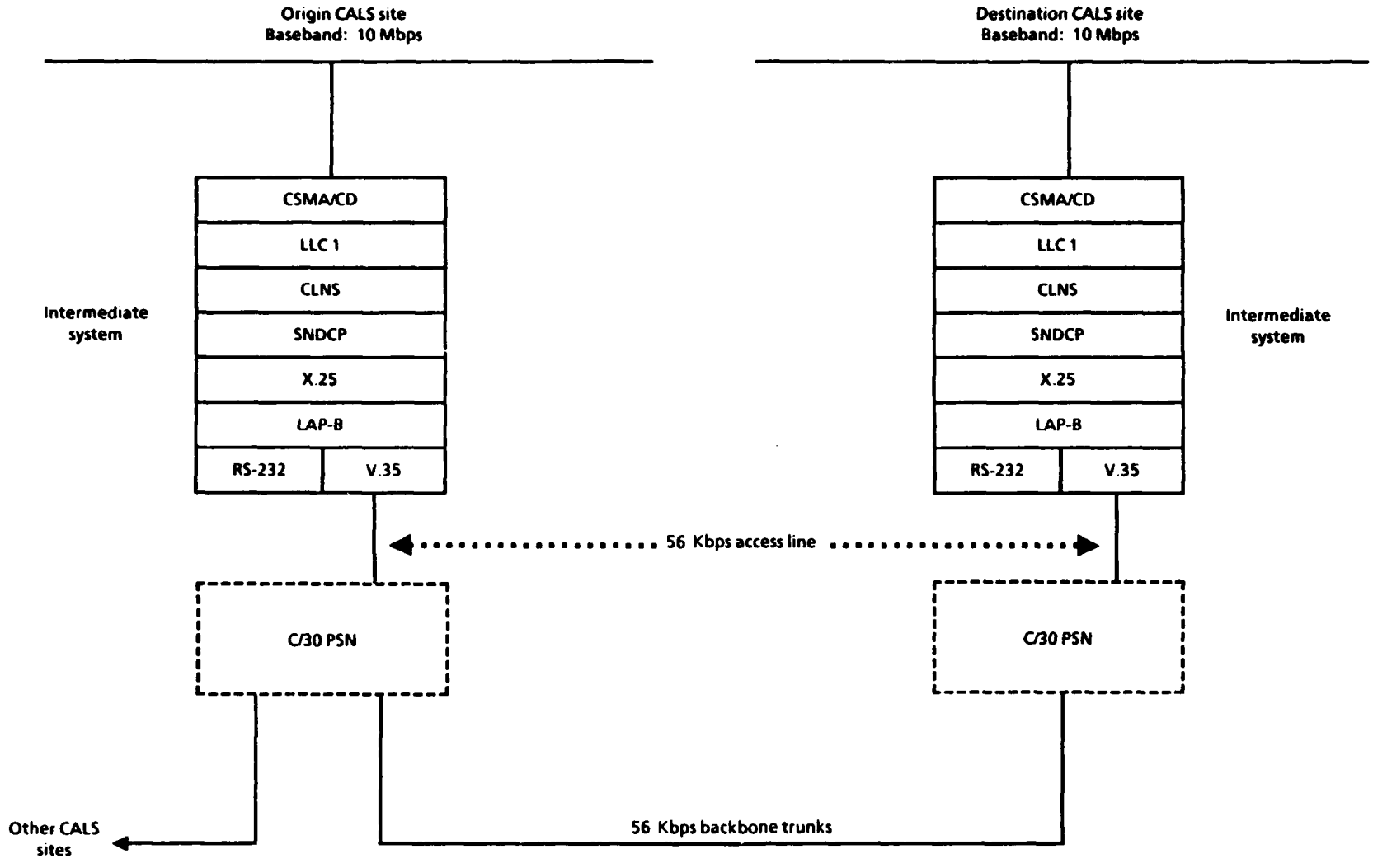


FIG. A-6. DDN CALS CLOSED COMMUUNITY

Until the required dynamic routing protocols are incorporated into the architecture, vendors must provide the mechanisms to accomplish static routing and the appropriate service interfaces to modify routing parameters and tables. Vendors must also contractually agree to migrate to the specified standards when these standards are accepted by NIST.

One or more intermediate systems, depending on any requirements for redundancy, must be provided to allow connectionless LANs to interface with the connection-oriented X.25 DDN network. Requirements for dual homing must also be considered at this point. The protocol architecture of the internetworking unit consists of the following and includes both a LAN side and a long-haul network side:

- LAN Subnetwork Access
  - Media Access: CSMA/CD as specified previously
  - Data Link: IEEE 802.2 LLC 1 as specified previously
  - Network: CLNS as specified previously.
- Internetworking
  - SNDCP: SNDCP provides the capability to map between the CLNS primitives and parameters and the DDN-specified X.25 implementation primitives and parameters. The implementation of SNDCP is to follow the ISO 8473 AD1 and conform to the NIST implementation recommendations.
- Long-Haul DDN Network Subnetwork Access
  - Network: The Network Access Protocol should be CCITT X.25 PLP, in conformance with DDN document *X.25 Host Interface Specification*, as previously specified.
  - Data Link: The Data Link Protocol should be CCITT HDLC LAP-B, in conformance with DDN document *X.25 Host Interface Specification*, as previously specified.
  - Physical: The interchange circuit should operate at 9.6 Kbps or 56 Kbps, in conformance with Military Standard (MIL-STD)-188-114-A balanced interface specification, as previously specified.

1.3.2.2 Gateway to Present DDN Systems. If a CALS project requires interoperability with other activities that have DDN protocol implementations (TCP/IP, FTP, SMTP, etc.), the project should use the appropriate DDN/OSI protocol

gateway. The intermediate system required to support communications between end systems using ISO protocols (i.e., nodes on the LAN) and end systems using the present DDN suite of protocols can be considered a full gateway system. This gateway system will require the ability to translate between all layers. NIST has developed a DDN/OSI protocol application gateway. This gateway provides a means to convert between the DDN FTP and the ISO FTAM Protocol, and between the DDN SMTP and the CCITT X.400 Protocol. Figure A-7 depicts use of the NIST application gateway. The following papers have been developed by NIST regarding the protocol application gateways:

- ICST/SNA-86-6 – A Gateway Architecture Between FTP and FTAM
- ICST/SNA-86-11 – A Gateway Architecture Between SMTP and X.400 MHS.

Since this gateway will impose a great deal of overhead to accomplish interoperability, its use should be minimized. Extensive use of the NIST gateway is not an acceptable means of providing interoperability for several reasons: (1) the task of protocol conversion is complex and requires a great amount of processing power, resulting in application performance and throughput degradation; (2) gateway conversion is expensive because of the additional hardware and software required; and (3) the gateway approach limits the amount of higher functionality that can be provided.

1.3.2.3 Gateway to Vendor-Unique Systems. If a CALS project requires interoperability with activities that have implemented communications over the DDN on the basis of a proprietary set of vendor upper-layer protocols, it should obtain the appropriate gateway intermediate system. The intermediate system required to support communications between end systems which use ISO protocols (i.e., nodes on the LAN) and end systems using a vendor-unique proprietary suite of protocols can be considered a full gateway system. This gateway system will require the ability to translate between protocols at all layers supporting vendor-unique communications and the OSI layers. The DLA Network (DLANET), an IBM bisynchronous-based network connected to the X.25-based DDN, requires a gateway of this type.

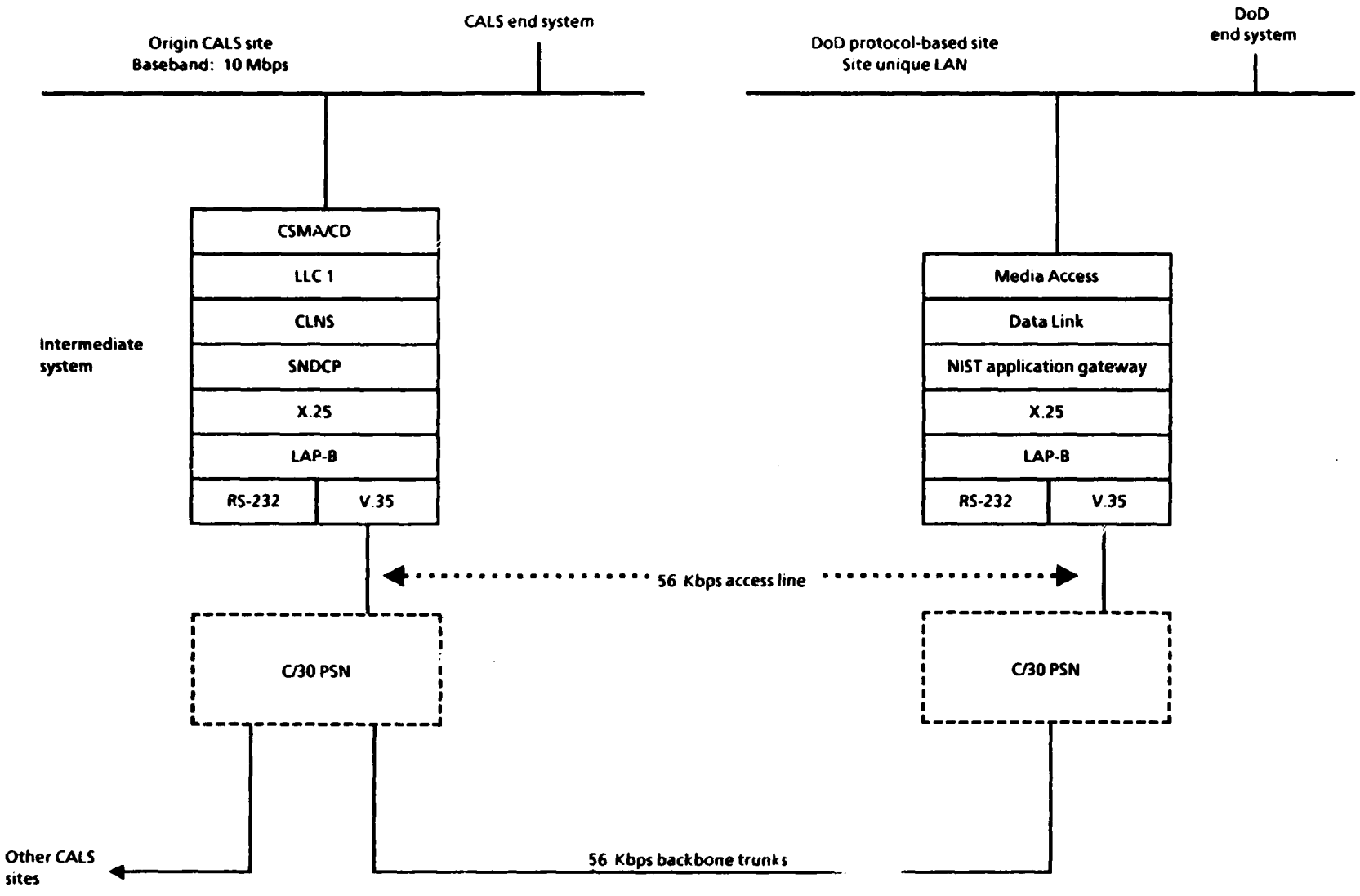


FIG. A-7. CALS GOSIP INTERCONNECTION WITH DoD-BASED SITES OVER DDN

1.4 Security Implications

The following section discusses near-term communications security protocols in both the local and long-haul environment.

1.4.1 LAN Security

Network security in a LAN will be restricted to the Data Link Layer (Layer 2) since, by its very nature, a LAN employs selection of messages by the MIU at Layer 2 rather than routing or switching at the Network Layer (Layer 3). Therefore, security mechanisms are more appropriately placed in either the DTE or the MIU itself.

Encryption-capable MIUs are on the market and in use in some DoD LANs. These units use an encryption algorithm based on the Data Encryption Standard (DES). Until the National Security Agency (NSA) announces a new encryption standard and manufacturers respond, LANs that require some measure of trustworthiness should use these off-the-shelf products.

Encryption devices should be integrated into all MIUs on a LAN requiring secured access. LANs operating in an unsecured environment may use these devices to provide "privacy" of information at the unclassified level. In a closed, environmentally secured LAN environment, the distribution and assignment of keys to different user groups can create "mandatory access" security levels, whereby access to information is controlled in a hierarchical manner.

1.4.2 DDN Security

DDN security, in the near term, will consist mainly of KG-84As. The KG-84A is an end-to-end encryption device situated between a host and a C/30 PSN or Interface Message Processor (IMP). The source and destination hosts can agree to a unique encryption key not available to other hosts. Different keys are used for each security level. Keys may also be issued on a community basis. In order for this encryption technique to work and still preserve routing control information for the PSN, the KG-84A contains sufficient intelligence on the DoD/IP to not encrypt the IP header.

KG-84A devices are generally used on all backbone trunks and on all access lines to classified DDN subscribers. KG-84As should be used on CALS projects

processing classified data. Unclassified users may also use this security mechanism to provide security level separation through the use of different keys for each level.

1.5 Vendor-Provided Capabilities

Because the near-term protocol suite is lacking in some fundamental areas, the vendor must provide solutions that can be used in the interim. A contractual agreement should be obtained stating that the vendor will migrate to the standards upon their incorporation into the GOSIP baseline. The following capabilities will need to be provided through vendor solutions:

- *ES-to-IS.* Vendors must provide a solution that allows end systems to route information to other end systems via an intermediate system. Required service interfaces must be provided to allow an operator to change routing tables. This solution will remain in place until the ISO ES-to-IS standard is accepted by NIST and incorporated in the architecture during the mid-term phase.

- *Block mode terminal protocol.* Vendors must provide a solution that supports the presentation of block mode terminal data on the display workstations, engineering workstations, etc. This solution will remain in place until the Forms/Image/Graphics Classes of VTP are accepted by NIST and incorporated into the architecture.

- *Network management.* Network management in the near term is to be provided by the vendor, because of the lack of ISO network management standards. The vendor must commit to migrating to the ISO networking management standards as they become available. In the interim, the vendor must provide three types of management services and service interfaces to the applicable protocol layers:

  - Configuration management entails the determination and control of the state of the networked system, that is, the logical and physical configuration or topology of the networked system. The functions provided must allow the network manager to monitor and control the arrangement and state of the network and its elements. Specific functions include

    - Addition/deletion of network resources
    - Determination/setting of parameters and characteristics
    - Initialization/termination of resources.

  - Performance management entails the control and assessment of the performance of the nodes, backbone media, and network operation. The functions provided must allow the network manager to collect and

analyze network measurement statistics and adjust performance by reconfiguring the network. Specific functions include

- Collection of statistics and measurements for throughput, response time, resource availability, and error rates
- Analysis algorithms to determine corrective actions or adjustments required to maintain or enhance performance.

- Fault management entails the detection and diagnosis of failures by using tests initiated by the network manager or by equipment with enough intelligence to notify the network manager of a failure. The functions provided must allow the network manager to detect, correct, and recover from failures in the network and/or its resources. Specific functions include
  - Confidence testing to determine the functionality of the network and its resources
  - Fault detection, notification, and isolation
  - Fault recovery.

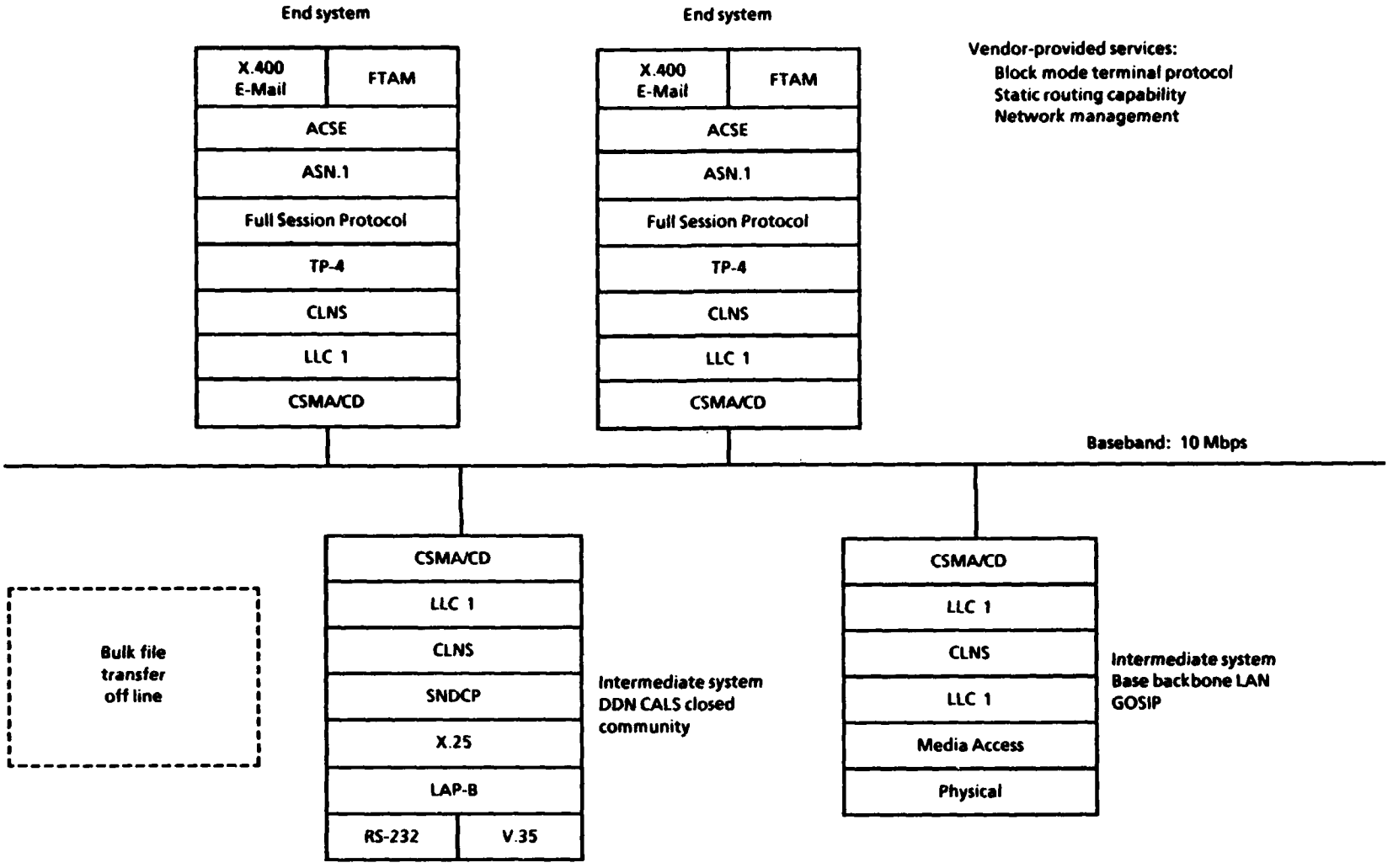
Network management and the control center/node must be provided to accomplish the above-listed functionality. This is to be comprised of a management console and any required diagnostic equipment.

1.6 Industry Interfaces

In the near term, any requirements to transfer data between CALS projects and private industry concerns should be accomplished in an off-line mode using optical disks, magnetic media, hard copy, etc., via overnight mail. Off-line media are the most cost-effective methods for distributing large volumes of CALS data. Standard data exchange protocols and procedures should be followed when using off-line methods of communication. Dedicated leased-line facilities between industry and a CALS project will be allowed only in exceptional cases during this time frame.

1.7 Summary of Near-Term CALS Communications

Figure A-8 summarizes the near-term communications capabilities. It depicts an ideal local environment in which the protocols implemented in the base or campus LAN are based on the OSI protocols and the GOSIP baseline, eliminating the need for a full gateway system. Connectivity to the DDN is provided, but use is limited to



Note: ACSE = Associative Control Service Elements; ASN.1 = Abstract Syntax Notation; CLNS = Connectionless Network Service; LAP-B = Link Access Procedure Balanced; LLC 1 = Logical Link Control Class 1; Mbps = Megabits per second; SNDCP = Subnetwork Dependent Convergence Protocol; TP-4 = Transport Protocol Class 4.

FIG. A-8. NEAR-TERM CALS COMMUNICATIONS (1989 – 1990)

high-priority/low-bandwidth transmissions. All bulk file transfer to and from industry and other Government users will be accomplished in an off-line mode.

1.8 Transition to Mid-Term Objectives

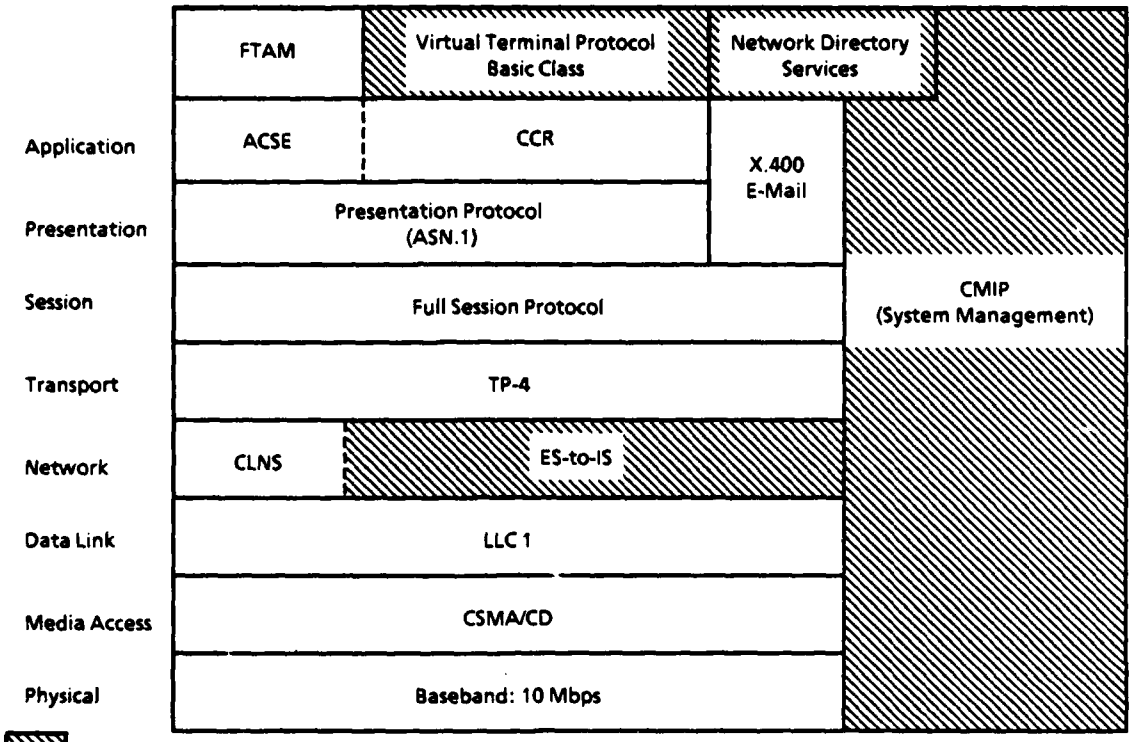
Transition to the mid-term phase should coincide with a major software upgrade from the vendor(s). It is important for the project manager to understand thoroughly each vendor's plans to upgrade equipment and/or software, and how the vendor's upgrades will affect various user-designed and -developed applications. The project manager should understand the compatibilities and incompatibilities of versions of the software in order to determine the level of effort required to convert existing applications. It is recommended that a contractual agreement with the vendors be made to ensure future releases are compatible with existing near-term-procured equipment and software. Before implementation of the mid-term phase enhancements and additions, conformance testing and interoperability testing will be required. Testing with user-designed and -developed applications will be completed before the transition occurs. A capacity analysis should be completed to determine whether additional subscriber links are required to support any increase in data traffic projected for the mid term.

2.0 MID-TERM COMMUNICATIONS (1991 – 1992)

The additional functionality to be provided in the mid term revolves around the addition of several new protocols, as well as enhancements and additions to the near-term-specified protocols. A dynamic internetworking capability is to be added during this time frame. End-system protocols were specified in the near term. The mid-term phase adds the capability to route dynamically between the end systems and the intermediate system supporting interconnection to the DDN or a base/campus LAN. Further capability will be available through optional use of the FTS-2000 network, which should be implemented by 1991.

2.1 Protocol Additions/Enhancements

Figure A-9 depicts the CALS end-system protocol architecture to support CALS projects in the mid term. Figure A-10 depicts the intermediate system that will be required. The following additional protocols should be implemented by vendors by the end of the mid-term time frame.



Note: CCR = commitment, concurrence, and recovery; CMIP = Common Management Information Protocol.

FIG. A-9. CALS MID-TERM PROTOCOLS (1991-1992) – END SYSTEM

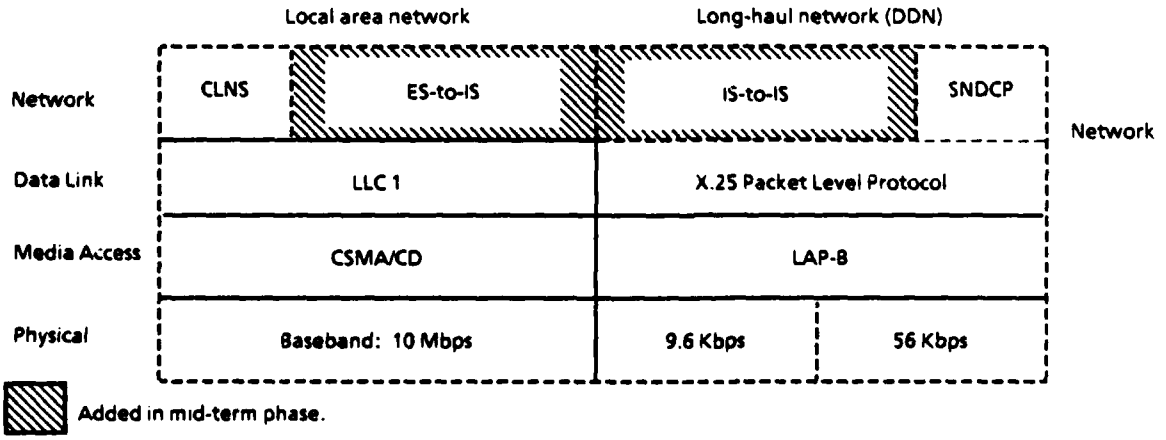


FIG. A-10. CALS MID-TERM PROTOCOLS (1991-1992) – INTERMEDIATE SYSTEM

2.1.1 Network Layer

The implementation of the following two dynamic routing protocols will greatly enhance the survivability of the internet. These protocols are used to keep member nodes informed of the state of the network. Through the exchange of these management protocols, intermediate systems (gateways) and end systems are informed of a failure, and traffic is redirected to an available alternate gateway or link. When the failure is corrected, a similar management exchange is used to inform gateways and systems.

The ES-to-IS protocol determines which routing tables are to be used for subnetworks supporting the source and destination end systems. The ES-to-IS protocol provides the capability for an origin end system to route its data dynamically to an intermediate system for transmission to a destination end system that resides in a different network. The ES-to-IS protocol (ISO DP 9542 ES-to-IS Routing Exchange Protocol) provides a mechanism to exchange configuration information and route redirect information.

The IS-to-IS protocol determines which routing tables are to be used among intermediate systems. The IS-to-IS protocol (ISO WD IS-to-IS Routing Exchange Protocol) allows intermediate systems to inform each other of their individual connectivity status and provides the exchange of net-reachability information among these systems. NIST is currently working with independent vendors and the MITRE Corporation to develop a proposal in this area. The international standard is expected to be formalized in 1990.

2.1.2 Application Layer

Enhancements to near-term application protocols and the addition of newly developed application protocol standards should also be accommodated during the mid-term phase. The ISO DIS 9805 commitment, concurrence, and recovery (CCR) functionality should be added to near-term implementations of CASE.

The ISO VTP Basic Class Standard is built around an object-based model that represents a terminal as a collection of arrays. Each array may contain a single element. This Basic Class VTP provides a command line type of capability with simple scrolling and is analogous to the DoD TELNET Protocol. It can be expected that VTP will be enhanced to accommodate forms-type applications in the future.

The following ISO Application Layer standards are to be implemented by CALS projects, in accordance with the NIST workshop agreements and the GOSIP baseline:

- ISO DP 9040 VT Basic Class Service, Part I
- ISO DP 9041 VT Basic Class Protocol, Part II.

2.1.3 Network Management

Incorporation of the ISO-specified management services and protocols should be accomplished during this phase. Implementation of these standards should replace vendor-unique solutions implemented in the near-term phase. The two major components of OSI management are systems management and layer management. Systems management deals with the control, monitoring, etc., of situations involving multiple layers. Layer management deals with the control, monitoring, etc., of situations involving a single layer. The Common Management Information Protocol (CMIP) is designed to provide the interface between layers for management message exchange. The layer management functions are to be incorporated into the CALS architecture in the long-term phase. The following ISO standards and documents are applicable to the management standards that are to be implemented by CALS projects, in accordance with the NIST workshop agreements and the GOSIP baseline:

- ISO CMIP
  - ISO DP 9595/1 Management Information Service Definition
  - ISO DP 9595/2 Common Management Information Service Definition
  - ISO DP 9596/1 Management Information Protocol Specification
  - ISO DP 9596/2 Common Management Information Protocol.

2.1.4 Directory Services

The following ISO Directory Services should be incorporated into the CALS architecture in the mid term. These services should be implemented on the basis of NIST workshop agreements and the GOSIP baseline:

- ISO DP 9594/1 Directory Overview – Concepts and Services
- ISO DP 9594/2 Models
- ISO DP 9594/3 Abstract Services Definition

- ISO DP 9594/5 Protocol Specification
- ISO DP 9594/6 Selected Attribute Types
- ISO DP 9594/7 Selected Object Classes.

2.2 Internetworking

This section addresses concerns for mid-term internetworking in both the local and long-haul environments.

2.2.1 Local Environment

All end systems must be modified to support the dynamic routing management protocol, ES-to-IS. All intermediate systems must be modified to support the IS-to-IS routing management protocol.

2.2.2 Long-Haul Environment

All packet-switching gateway nodes within the DDN should, by 1991, support these dynamic routing protocols. This capability will allow routing management information to be passed among systems, permitting routing to be based on the present condition of the internet (e.g., inoperable links or nodes). This will replace the static method of determining routing paths implemented in the near term.

The ISO and DoD protocols should coexist by 1991, allowing use of the Mini-TACs to support remote terminal connectivity to DDN and any subsequent CALS host processor. Terminal connectivity will be restricted by the limited functionality provided by the VTP Basic Class Protocol to be implemented in this time frame. This protocol, functionally equivalent to the present DoD TELNET protocol, provides support for scroll-mode, line-at-a-time terminals only.

On the basis of performance of the near-term-specified physical circuits and additional long-haul transmission requirements, it may be necessary to add additional links or upgrade subscriber links to a higher bandwidth. Requests for additional bandwidth must be made to DCA as soon as requirements are known or performance is determined to be unsatisfactory. Appendix B, Network Capacity Planning, will aid in determining the additional bandwidth required.

2.2.3 DDN Tariff Implementation

It is anticipated that, during the mid term, a use charge-back tariff will be put into place by DCA. The DDN tariffs for cost recovery, scheduled for FY90, are presented in Table A-1.

TABLE A-1

PROJECTED DDN TARIFF (MILNET)

Line speed		Hosts	Terminals
56/50 Kbps	single	$2,200	$300
	dual	2,800	390
19.2 Kbps	single	1,650	300
	dual	2,100	390
9.6 Kbps	single	1,050	300
	dual	1,350	390
4.8 Kbps	single	850	300
	dual	1,100	390
2.4 Kbps	single	700	300
	dual	900	390
1.2 Kbps	single	500	300
	dual	650	390
0.3 Kbps	single	300	300
Dial-up service		7.5 cents per minute	
Traffic charge per kilopacket		Peak hours	Off-peak hours
Precedence 1		$1.35	$1.05
Precedence 2		3.00	3.00
Precedence 3		4.00	4.00
Precedence 4		5.00	5.00

Note: MILNET = Military Network; single = single access to DDN; dual = dual access to DDN; Precedence 1 – 4 = the priority of the user's traffic with Precedence 4 being the highest priority.

Since the kilopacket charge will be based on packets of any size, the maximum packet size of 1,024,000 octets or bytes should be used. This number may be adjusted, depending on throughput and retransmission. Off-peak time use of the DDN is recommended for the transmission of nontime-critical data, because of the substantial reduction in cost. The costs of the DDN are expected to be competitive with those of commercial packet networks.

2.2.4 Industry Interface

During the mid term, transmission of a small portion of the information required to be transmitted between industry and a CALS project can be accomplished over the DDN or a public PSN. The specific CALS project must sponsor the industry vendor for inclusion in the DDN internet. A careful analysis of real-time data transmission requirements must take place, given the bandwidth limitations of the DDN and the costs of on-line transmission. Only inquiry-type traffic and high-priority/low-bandwidth transmissions over the DDN should occur in this time frame. Major defense industries have embraced the Technical Office Protocol (TOP) suite for use in the office and laboratory environments, or the Manufacturing Automation Protocol (MAP) in the factory environment, and should have migrated to Version 3.0 of the respective standard by the mid-term phase. The TOP/MAP Version 3.0 and the protocols implemented in this plan will be interoperable. The mechanism to accomplish real-time transmission of information should be DDN or a public packet-switching X.25-based network. Bulk information and proprietary or sensitive data should be transmitted off-line.

2.3 Security Implications

2.3.1 LAN Security

Under the umbrella of the NSA Commercial COMSEC[1] Endorsement Program (CCEP) for highly secured encryption products, prototypes of some promising devices will become available during this period. Mass production should follow about a year after prototype debut. These modules will be in the form of cards that can be conveniently integrated into an existing MIU, or will be marketed as options on MIU boxes. Both will provide cryptographic services and key management capabilities.

[1]Communications Security.

One manufacturer plans to offer two model types: one for the classified COMSEC marketplace and the other for unclassified "sensitive."

It is recommended that LANs requiring confidentiality incorporate the use of these COMSEC encryption devices into all MIUs.

2.3.2 DDN Security

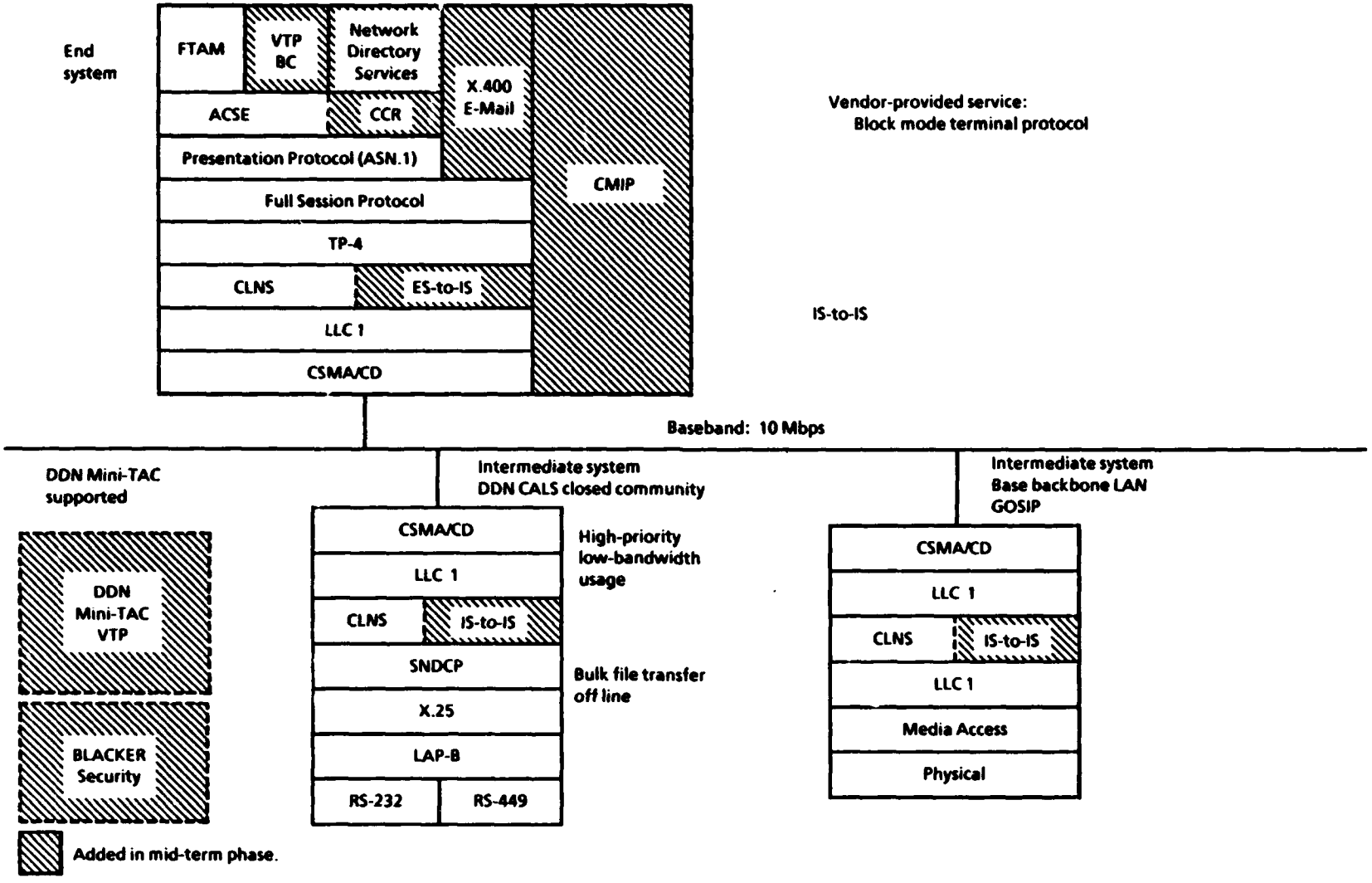
The BLACKER encryption methodology is expected to become available during the mid-term period. BLACKER is dependent upon DoD/IP. Unless BLACKER's design specifications are augmented to accommodate ISO/IP's differing header, end-to-end encryption will be possible only for those hosts still employing the old DoD protocol suite. As DCA has mandated this period for full coexistence of the DoD and ISO architectures, we expect that BLACKER will be retrofitted to support both DoD/IP and ISO/IP before its debut. It is also expected that BLACKER will coexist with KG-84A devices for the mid-term duration.

2.4 Summary of Mid-Term Communications

Figure A-11 depicts the CALS mid-term communications architecture. The major additions to the CALS architecture at this point are the dynamic routing and network management protocols, and VTP. The DDN should also introduce at this time the Mini-TAC incorporating VTP to support inquiry and mail-type applications for remote CALS users. BLACKER security should also become available during this period. The DDN probably will not yet have converted to a T-series-based network, so use will still be restricted to high-priority/low-bandwidth transmissions.

2.5 Transition to Long-Term Objectives

Transition to the long-term phase should coincide with a major software upgrade from the vendor(s). It is important for the project manager to understand thoroughly each vendor's plans to upgrade equipment and/or software, and how the vendor's upgrades will affect various user-designed and -developed applications. The project manager should understand the compatibilities and incompatibilities of versions of the software in order to determine the level of effort required to convert existing applications. It is recommended that a contractual agreement with the vendors be made to ensure future releases are compatible with existing near- or mid-term procured equipment and software. Before implementation of the long-term phase enhancements and additions, conformance testing and interoperability testing



Note: ACSE = Associative Control Service Elements; ASN.1 = Abstract Syntax Notation; CCR = commitment, concurrence, and recovery; CLNS = Connectionless Network Service; CMIP = Common Management Information Protocol; LAP-B = Link Access Procedure Balanced; LLC 1 = Logical Link Control Class 1; Mbps = Megabits per second; SNDCP = Subnetwork Dependent Convergence Protocol; TP-4 = Transport Protocol Class 4; VTP BC = Virtual Terminal Protocol Basic Class.

FIG. A-11. MID-TERM CALS COMMUNICATIONS (1991 – 1992)

will be required. Testing with user-designed and -developed applications will be completed before the transition occurs. The long-term phase will add the higher bandwidth media required to support the CALS data transfer requirements. The individual CALS projects should plan to use T1 (1.544 Mbps) subscriber links to the DDN, begin to migrate to the Integrated Services Digital Network (ISDN), or use the Defense Commercial Telecommunications Network (DCTN), as alternatives for higher bandwidth requirements. Existing physical links can be replaced with customer premises equipment (CPE) and T1 subscriber links where required. The hardware and software to accommodate these two alternatives are to be obtained from DCA or the applicable Bell Operating Company (BOC).

3.0 LONG-TERM COMMUNICATIONS (1993 – 1994)

The long-term enhancements to the previously implemented CALS communications architecture involve implementation of several application layer protocols and the transition to a higher bandwidth medium at the Physical Layer. The CALS project manager should track efforts to standardize the following protocols and keep abreast of the status of the following transmission media. Other protocol standards not listed here may become important in the future and should be added if necessary.

3.1 Additional/Enhanced Protocols

Figure A-12 depicts the end-system protocol architecture to support the CALS projects in the long term. Other protocols may be added if required to interface with the emerging transmission technology.

- Application protocols.
  - Virtual Terminal Protocol. The ISO/OSI terminal-oriented protocols that will provide communications among heterogeneous terminals and applications are to be incorporated at this time. Forms Class should be standardized and incorporated at this point. The Forms Class standard (ISO 9040/9041 Forms Class) will provide block mode terminal support.
  - Video Text Protocol. The Video Text Protocol (ISO Video Text Services) will provide the support required for the transfer of video data used in automated publishing and other applications required by the CALS projects.

- Layer management. The ISO and IEEE standards groups recommendations and specified standards are to be incorporated into the CALS architecture at this time. The following will be greatly enhanced before long-term implementation:
  - IEEE 802.1 Part B Systems Management Protocol
  - IEEE 802.1 Part B Systems Load Protocol
  - IEEE 802.3 Layer Management
  - IEEE 802.2.3 LLC Sublayer Management.

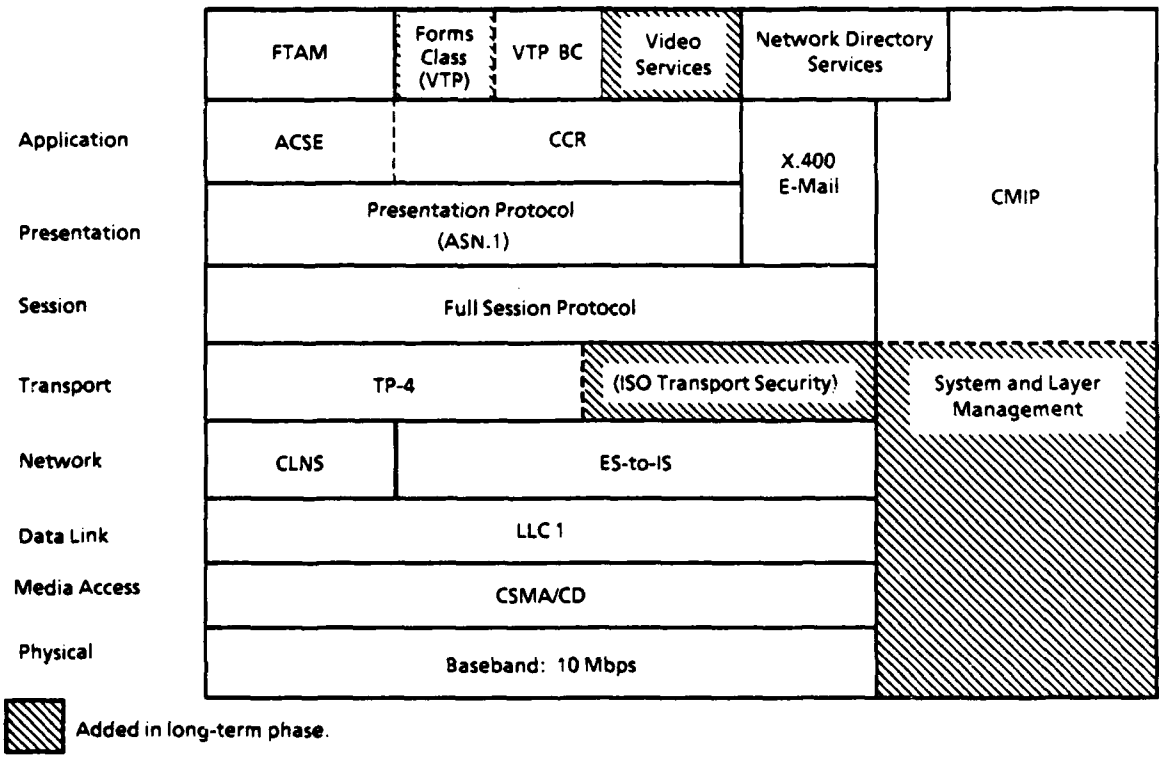


FIG. A-12. CALS LONG-TERM PROTOCOLS (1993 – 1994) – END SYSTEMS

3.2 Long-Haul Environment

The long-term phase will include the addition of the physical media required to support on-line transfer of bulk file data associated with CALS projects. Figure A-13 depicts the intermediate system to support this added bandwidth capability.

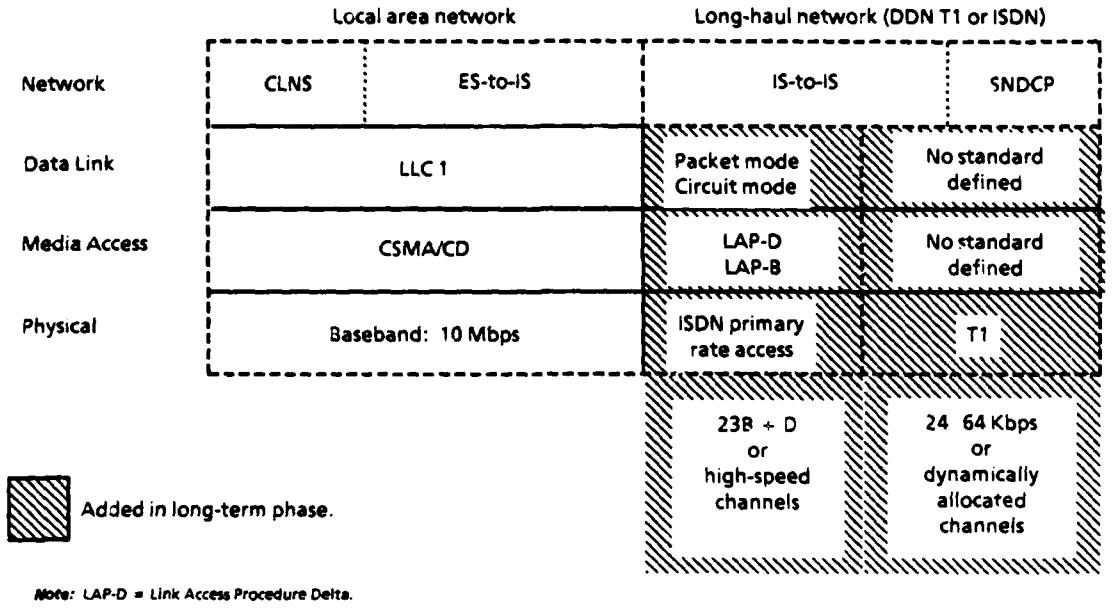


FIG. A-13. CALS LONG-TERM PROTOCOLS (1993-1994) – INTERMEDIATE SYSTEM

3.2.1 Defense Data Network

It is anticipated that the DDN will begin to offer T1 capability by 1994 for both subscriber access links and backbone trunks. The increased bandwidth will allow the DDN to support larger volumes of CALS data transmission workloads. CALS projects whose volumes dictate the increase in bandwidth should consider migrating to the T1 service if it is available.

The T1 composite data rate can be used in its entirety or can be separated into channels. The most common channeling scheme divides the T1 composite into 24 channels, each capable of carrying 64 Kbps. Each 64 Kbps channel is designated as DS0, and the entire 24-channel composite is designated as DS1.

3.2.2 Integrated Services Digital Network Services

If the DDN has not upgraded to T1 service by this time, ISDN should be examined as an alternative. ISDN will provide two broad categories of services, Teleservices and Bearer (B) services.

Teleservices involve the upper layers of the OSI model (Transport Layer and above). Services to be provided include teletex, videotext, and electronic mail.

Teleservices are still in the process of being defined by the CCITT. It is not known how these services will relate to or interact with the higher level protocols defined by ISO. It is expected that much of the work being done by ISO will be incorporated into the ISDN Teleservices specifications.

B services involve the lower layers (Physical through Network) of the model. Two basic B services will be offered by ISDN: Circuit Mode Information and Packet Mode. Circuit Mode Information is 64 Kbps Unrestricted Digital Information (UDI); it is used in such applications as speech and audio transmission. Circuit Mode also supports varying bandwidths to accommodate different types of data ranging from 364 Kbps to 1,920 Kbps. Circuit Mode will accommodate the bulk file transfer requirements of CALS projects. Packet Mode supports transfer of user data through either virtual call switched circuits or permanent virtual circuit services. Virtual call service entails setting up and tearing down the circuit for each call; it is analogous to dial-up service. Permanent virtual circuits remain established until changed by a network administrator; they are analogous to dedicated lines. The access protocol for virtual circuit service is Layer 3 of CCITT standard X.25. It is the user's responsibility to package the data; ISDN will not alter the data. Packet Mode service will provide transaction-oriented processing required by CALS projects.

Two types of subscriber access to the ISDN are anticipated: Basic Access and Primary Access. The Basic service interface consists of two 64 Kbps B channels and one 16 Kbps Delta (D) channel. This is known as 2B+D access. The B channels transmit bidirectional digital voice and/or data traffic, while the D channel carries signaling for call set up, call clearing, etc. Both the B and D channels can also be used for packet-switched data applications. The Basic service will be oriented toward residential and small business subscribers.

The Primary Rate Interface is used for connecting local premise distribution systems to the ISDN. It provides a transmission bandwidth of 1.544 Mbps. Known as 23B+D, the Primary Rate Interface consists of 23 B channels and a single D channel, all operating at 64 Kbps. Because of the limitations of current T1 technology, 8 Kbps of each channel are required to support timing overhead. Thus the effective throughput of each 64 Kbps channel is only 56 Kbps. One of the requirements of ISDN, known as clear channel capability, is that all 64 Kbps of each channel be usable by a subscriber. Higher speed applications such as teletex, videotext, and electronic mail can be served via Higher Speed Channels (H channels). The

H0 channel provides a bandwidth of 384 Kbps; the H11 channel provides 1,536 Kbps. Various combinations of H and B channels can be configured by the end user.

The CCITT ISDN standards (I-Series) began with the *Red Book* issued in 1984. The *Red Book* stated the basic architectural model and the types of services that were to be offered. The next milestone was the *Grey Book*, issued in 1986. It contained the specifications for Layers 1 and 2. The next specification, the *Blue Book*, has been circulated on a tentative basis but awaits official approval. The *Blue Book* will contain the complete specifications for Layers 1, 2, and 3 (Physical, Data Link, and Network) and should be followed by vendors supporting CALS projects.

CCITT has recommended ISDN standard access protocols for Layer 1 through Layer 3 of the model. If ISDN interconnection is implemented, then the Primary Rate Interface should be specified rather than the Basic Rate Interface. This interface should replace the long-haul network side of the intermediate system gateway already implemented.

The Network Layer provides the means to establish, maintain, and terminate network connections across an ISDN among communicating application entities. This layer will support both Circuit Mode and Packet Mode ISDN. Packet Mode is to be used for transaction-oriented, packet-switched applications, while Circuit Mode will be used for bulk file transfer. The two applicable CCITT standards are

- CCITT I.462/X.31 Support of X.25 DTEs
- CCITT I.451/Q.931 ISDN Network Protocol.

The Data Link Layer encompasses the specifications and procedures for transferring messages between Layer 3 end users on the D channel. The CCITT I.441/Q.921 ISDN Data Link Protocol standard is applicable.

The Physical Layer reflects the ISDN's digital connectivity. CCITT recommends two physical access interfaces: the basic rate access (2B + D) and the primary rate (23B + D).

- Basic Rate Interface. The channel structure is two B channels (64 Kbps each) and one D channel (16 Kbps), with a total bit transmission rate of 192 Kbps, including 48 Kbps of overhead. This interface supports both point-to-point and multipoint configurations and uses a two-pair (4-wire) interface. The CCITT I.430 Basic Rate Interface standard is applicable.

- Primary Rate Interface. The digital carrier T1 is used for Primary Rate Interface. This interface supports point-to-point operation only. The 1.544 Mbps transmission rate supports clear channel capability by using out-of-band signaling. The channel structures expected to be supported are
  - Twenty-three B channels (64 Kbps each) and one D channel (64 Kbps)
  - Up to four H0 channels (384 Kbps each) and one shared D channel
  - One H11 channel (1,536 Kbps) and one shared D channel.

The CCITT I.431 Primary Rate Interface standard is applicable to the Primary Rate Interface.

3.3 Security Implications

3.3.1 DDN Security

In September 1986, ISO's Ad Hoc Group on Security released an addendum that recognized the need for an OSI security architecture. This draft provided general descriptions of security services and related security mechanisms, as well as discussed the possible placement of these mechanisms within the seven layers. Security services described include the following:

- Identification – of peer entity in protocol data unit.
- Peer entity authentication – is entity the one claimed?
- Access control – defines access rules to information.
- Data confidentiality – no unauthorized disclosure.
- Communications integrity – data received are data sent.
- Service availability – ensure minimum service levels.
- Accountability – ensure retaliatory threat.
- Nonrepudiation – receiver cannot deny receipt of data.

The following security mechanisms were described in the draft:

- Encipherment (encryption) – render data unintelligible via mathematical function
- Digital signature – "fingerprint" appended to enciphered data proving source and integrity of data unit

- Access control – authorized lists, passwords, security labels, etc.
- Data integrity – via the use of checksums, sequencing, timestamping, etc., ensure data have not been tempered
- Entity authentication – established via passwords or cryptographic means.

The trick is to apply the appropriate security mechanism at the appropriate protocol level to obtain the optimal security services at the lowest possible cost. Various papers have been presented arguing for placement of these security mechanisms at various levels. To date, no consensus has been reached by ISO on an architectural standard for network security. However, the available literature seems to point at either Layer 3 (Network) or Layer 4 (Transport) as the most likely place to impose security mechanisms.

Evaluation of network security is also in its infancy. It was only in mid-April 1987 that the Trusted Computer Security Evaluation Criteria (TCSEC) was extrapolated from its stand-alone computer origins to embrace networking complexities. This Trusted Network Interpretation (TNI), as it is now called, is still in its draft stage.

Although the BLACKER encipherment methodology holds much promise, there are some reservations. BLACKER's candidacy for A1 certification and its ability to operate with multisecurity levels, albeit within certain restrictions, makes it an attractive long-term security mechanism. However, BLACKER has been in development for quite some time; its anticipated implementation date is after 1989. BLACKER may be too complex to accommodate changes easily. A policy question arises: Given that DoD is dedicated to an eventual full OSI adoption, what will be the impact if ISO proclaims a network security standard that does not easily accommodate BLACKER?

CALS activities should be guided by an eventual ISO network security standard if that standard also meets the unique requirements of DoD. In spite of the reservations, BLACKER can probably be retrofitted to be compatible with the ISO standard. However, there are no clear indications regarding the form that the eventual ISO standard will take. Any proffered advice will be highly speculative at best. There are still questions about BLACKER that may not be answered because of its classified nature.

3.3.2 LAN Security

As with the long-haul DDN, the network architecture for LAN end systems will also be guided by the ISO network security standard. In this case, control of the cryptosystem is unlikely to be at the Data Link Layer, i.e., embedded in the MIU. Most probably, the network security architecture will fall under the auspices of the Network Layer or the Transport Layer.

This will have implications for personal computer (PC) end systems. Hopefully, COMSEC devices small enough to fit the PC will be available to provide the necessary security services.

APPENDIX B

NETWORK CAPACITY PLANNING

CONTENTS

		Page
1.0	Introduction	B-3
2.0	Workflow Definition	B-3
3.0	Network Access Resources	B-5
4.0	Application	B-7

NETWORK CAPACITY PLANNING

1.0 INTRODUCTION

Network capacity planning involves predicting the amount of network resources required to exchange an estimated amount and type of data within a particular period. This appendix provides sample throughput estimates for standard network resources. The variables that the Computer-aided Acquisition and Logistic Support (CALS) project manager must provide are the amount and type of data, or the workflow, and the period in which the transmission must take place. These variables can be further defined for CALS projects within the near term. The workflow will consist of interactive transactions and batch transmissions. The network access resources include various types of physical layer media that define the physical line speed of an individual link; the Data Link Layer, which determines how efficiently the individual physical link will be utilized; and the Network Layer, which determines network overhead.

2.0 WORKFLOW DEFINITION

A typical computer system communications workflow can be categorized either as interactive transactions or as batch transmissions. Interactive transactions consist of status inquiries, database updates, mail messages, etc. This type of workflow is normally generated by people working at interactive data terminals. The record sizes vary from 2 to 1,920 bytes. While this type of workflow is important to transaction processing systems, it is not significant when compared to the workflow required for batch transmissions.

Batch transmission consists of moving files or mail messages. Their transfer can be the result of either a background task or a transaction. The vast amount of CALS information can be attributed to technical data or engineering drawings. The CALS project manager will need to determine the total number of bytes for all files and diagrams to be transmitted and the period in which the transmissions must occur.

The (Navy) Engineering Drawing Management Information and Control System (EDMICS) project is used here as an example of capacity planning. Table B-1 lists engineering drawing types, their sizes, and occurrence percentages as provided by an analysis of the EDMICS project. These occurrence percentages should be modified by CALS project managers to describe their particular environment. The data size is derived by assuming a density of 40,000 bits per square inch. The average size is the product of the occurrence percentage times the data size.

TABLE B-1

EDMICS DIAGRAM DISTRIBUTION

Drawing size	Occurrence (percent)	Data size (million bits)	Average size (million bits)
A. 8½" x 11"	24	3.74	.9
B. 11" x 17"	16	7.48	1.2
C. 17" x 24"	14	14.96	2.09
D. 22" x 34"	14	29.92	4.19
E. 34" x 44"	4	59.84	2.39
F. 28" x 40"	4	44.80	1.79
G. 11" x 48"[a]	3	21.20	.64
H. 28" x 60"[a]	11	67.20	7.39
J. 42" x 100"[a]	2	201.60	4.03
Other (A Size)	8	3.74	.30
Total	100	454.48	24.92

[a] Variable-length paper (average length estimated): G = 11" x 22" to 90"; H = 28" x 42" to 142"; J = 42" x any length.

Applying a compression ratio of 10:1 reduces the transmission requirement for an average drawing to 2.5 Megabits (Mb) and the transmission requirement for a large drawing to 20.1 Mb. It is predicted that an annual total of 14,416,200 drawings will be transmitted in response to user requests for the entire EDMICS project. Dividing the annual volume by an assumed workyear of 261 days results in an average of 55,234 drawings to be transmitted each workday.

It is estimated that 5 percent of this traffic (2,762 drawings per day) will be generated by remote users. The remainder (52,472 drawings per day) will be generated by local users on the CALS functional local area network (LAN).

These figures do not take into account traffic distribution habits for a typical workday. Some systems, such as bank teletex systems, transmit the majority of their traffic at the end of the day. It is not rare for some networks to have as much as 90 percent of their traffic occur during a specific 1- or 2-hour period of the workday. We will assume for our planning that 80 percent of the traffic for the repository in question will need to be processed in a 4-hour period. This produces the following workflow requirements:

- *Remote Access*
  - 2,762 drawings × 80 percent = 2,210 drawings (peak load)
  - 2,210 drawings ÷ 4 hours = 553 drawings per hour
  - 553 drawings per hour × 2.5 Mb per drawing = 1,383 Mb per hour.
- *Local Access*
  - 52,472 drawings × 80 percent = 41,978 drawings (peak load)
  - 41,978 drawings ÷ 4 hours = 10,495 drawings per hour
  - 10,495 drawings per hour × 2.5 Mb per drawing = 26,238 Mb per hour.

3.0 NETWORK ACCESS RESOURCES

CALS projects must primarily use the Defense Data Network (DDN) for remote access. The highest speed access circuit to the DDN presently available is 56 Kilobits per second (Kbps). Estimating the time it will take a drawing to be transmitted over a 56 Kbps line must take into account the combined DDN and X.25 packet network overhead. This overhead consists of extra bits added to each packet for protocol control information and error detection. Data passing between DDN packet-switching nodes (PSNs) are subject to processing and queuing delays. Packet transmission times increase with each 56 Kbps link in the total path (subscriber access lines between origin/sender and PSN, PSN to PSN – referred to as the backbone network – and the subscriber access line between the destination/receiver and the supporting PSN). This overhead is factored as an increase of 25 percent of traffic volume or as a reduction of line capacity to 70 percent of raw line speed.

The following formula approximates the number of raw data bits that a 56-Kbps DDN line can effectively transmit

.056 Mbps[1] × 70 percent (accounts for loss due to queuing delay)

× 80 percent (accounts for loss due to protocol data overhead)

× 3,600 seconds per hour = 113 Mb per hour.

It follows, then, that to accommodate remote access of 1,383 Mb per hour (divided by 113 Mb per hour per line) requires 12 lines at 56 Kbps each.

The above formula shows that the entire EDMICS project would require at least 12 56-Kbps DDN lines to handle a peak period. This is assuming that the traffic could be efficiently divided among the 12 lines. It is not feasible to expect a single 56-Kbps DDN backbone line or even two lines (assuming the data can be split over several paths) to service 12 56-Kbps subscriber access lines.

In summary, the near-term use of DDN for remote access to a CALS effort must be restricted to high-priority transmissions only. This example accounts for only one large EDMICS repository. When one considers the ramifications of the remaining 38 EDMICS sites and other CALS initiatives, the more obvious the need to limit near-term use of the DDN.

The long-term solution is for CALS to use T1 subscriber access links to DDN. This solution will require DDN to use T2 and above transmission links for the backbone network. A 1.544-Mbps T1 interface will provide the hourly throughput capability required by a CALS site with a workload similar to that in the above example.

Local access by a LAN is not as much of a problem. The following formula approximates the number of raw data bits that a 10-Mbps LAN can effectively transmit:

10 Mbps × 80 percent (accounts for loss due to queuing delay)

× 95 percent (accounts for loss due to protocol data overhead)

× 3,600 seconds per hour = 27,360 Mb per hour.

---

[1]Megabits per second.

It follows that to accommodate local access of 26,238 Mb per hour (divided by 27,360 Mb per hour per line) requires 1 LAN at 10 Mbps.

A single baseband 10-Mbps LAN will be sufficient to meet the local access requirements for this sample EDMICS repository or other CALS projects with similar workload requirements.

4.0 APPLICATION

In assessing the potential workflow for a CALS application, project planners need to look at numbers and types of potential system users as well as location and access of data repositories.

Critical attention must be paid to individuals such as engineers and technicians who would have demand for graphical data. By collecting this information, and estimating peak loading factors, it is possible for planners to determine points and level of demand.

The other primary consideration will be the potentially limiting capabilities of the system architecture as they affect the ability to move CALS data both to local and remote users. There will be a limit to the repository's capacity to service demand and the LAN's ability to function efficiently under a heavy traffic load. These and other items must be considered in planning capacities of CALS implementation.

APPENDIX C

INTELLIGENT GATEWAYS IN THE CALS ENVIRONMENT

CONTENTS

		Page
1.0	The CALS Focus of Intelligent Gateways	C- 3
2.0	The "External" View of CALS Data Access Requirements	C- 5
2.1	Overview of CALS Data Access Requirements	C- 5
2.2	Statement of the External View	C- 9
3.0	The "Internal" View of CALS Data Access Requirements	C-12
3.1	Gateway Services	C-14
3.2	Standards	C-16
4.0	Issues	C-16
4.1	Data Accessibility	C-17
4.2	Data Compatibility Issues	C-21
4.3	Data Control Issues	C-23
4.4	Transitioning Issues	C-25
4.5	Standards Issues	C-26
5.0	Approaches to Providing CALS Data Access Facilities: A Target Architecture	C-27
5.1	Standards	C-27
5.2	Logical Integration	C-28
5.3	CALS Framework	C-29
5.4	Object Orientation	C-31

INTELLIGENT GATEWAYS IN THE CALS ENVIRONMENT

The purpose of this appendix is to identify and explain the key issues and problems associated with access to heterogeneous data sources. The discussion focuses to some extent on semantic issues associated with providing integrated access to technical information. Problems arise in this area because the various information sources and recipients operate in different environments, with different purposes, and different requirements.

1.0 THE CALS FOCUS OF INTELLIGENT GATEWAYS

The CALS requirement for integrated access requires more than interconnection – it should allow the end user to transparently access data and to be able to interpret them. A successful intelligent gateway (IG) for CALS requires interoperation of distributed hardware and software in support of an end-user request for information. From the perspective of an end user, it should be possible to state a request for information in terms of the *purpose* of the request (e.g., as an on-line query) rather than in terms of a bulk data transfer; the request can then be satisfied by independent but cooperating interoperable systems in a way that directly responds to the user query and to the way the data will be used. A further characteristic of any IG effort should be modularity of implementation, as the underpinnings of the CALS system evolve.

Consider the following example. A data communications network can connect a user with a database and can transport the user's database requests and the data. But to use the database, the user must know in addition (1) what data are in the database; (2) how to gain access to the database; (3) how to query the database; and (4) how to interpret the results of the queries. The database may, for example, contain current warehouse stock, but it may be important for the user to know that the information is not really current but, in fact, a few days old.

It follows that issues such as "knowing how to interpret data" and "knowing how to interact with another application" are associated with the *meaning* of the information being transferred. It is important to distinguish between the issues of

preserving the meaning of data during their transport among different systems and determining the meaning of the transported data in the first place.

The function of Open Systems Interconnection (OSI) Layer 6 in preserving the meaning of data during transport has two aspects. First, as information is moved between applications, its storage format may be changed (for reasons of efficiency). Second, different applications may choose different ways of representing the same information (e.g., a zip code might be stored as a string of decimal characters in one application and as an internal binary number in another). As a result, information may have to be reformatted when it is exchanged. The purpose of OSI Layer 6, then, is to ensure the format changes do not change the meaning of the data themselves (e.g., that the binary number is indeed the equivalent of the decimal character string), to provide an architectural component for the reformatting services, and to allow the establishment of conventions regarding the format in which the information will be transported.

All this assumes that the data supplier's access tools and applications can provide the exact information the receiving application desires. But often, when a diverse array of applications with differing requirements is being supported, such information cannot be provided.

The above example illustrates two other issues that are associated with supporting data access (but which are not currently addressed by OSI Layer 6 or 7):

- Even if a format has been defined for transmitting information in a specific application area (such as orders and shipments, or document processing), the format may be inadequate to capture *all* information that a specific application program processes.
- Different applications may use different information to support the same activities (and the established data exchange format might not be adequate for all of them).

In summary, there is a difference between ensuring the information received is the same as what was sent, and ensuring (1) the source can provide the information that the recipient requires; (2) the recipient can understand and process the information sent; and (3) the transport mechanism can accommodate all information that needs to be exchanged. Integration is not possible without addressing these three issues.

The key to achieving long-term CALS goals is to establish a transition path that builds on basic interconnection services to achieve a gradual and logical integration of information sources as they become available. This transition path must occur within the context of a clearly defined target architecture in order to assess progress and to be able to make trade-off decisions in light of advancing technology or changing requirements. This target architecture must be developed from the perspective of the application requirements (a high-level view of the target) rather than that of how to interconnect existing systems (i.e., a bottom-up implementation approach).

2.0 THE "EXTERNAL" VIEW OF CALS DATA ACCESS REQUIREMENTS

A useful first step in defining the target architecture for CALS is to examine CALS long-term information accessibility goals from the end user's perspective. Such an "external" view describes the CALS architecture's functional requirements rather then its architectural components. From this view, we can then identify what functional components and approaches will best support the external requirements. Identifying these components and approaches provides an "internal" view allowing us in turn to identify the key technical issues that must be resolved. The "internal" view of CALS data access requirements will be described in Section 3 of this appendix; the "external" view is given below.

2.1 Overview of CALS Data Access Requirements

In the short term, the goal of CALS is to provide enough interface capability to support selected logistics infrastructure functions through direct electronic data transfer to a logistics database. This goal will be achieved by the adoption of standards to support interconnection of the sources and recipients.

The long-term goal is more ambitious: to provide *integrated* on-line or interactive access to logistics information, regardless of its source or location. This access will be to Government-owned, contractor-supported databases, as well as involving bulk transfer capability between Government and contractor data banks. Achievement of the goal will require providing automated, selective access to needed documentation where peculiarities regarding the documentation's source(s), format(s), and contents are handled by the system in a fashion transparent to the user. We focus in this section on the long-term goal.

2.1.1 Current Information Flows

Data exchange in the current information resource base is characterized by the following:

- Documentation important for supporting the logistics functions is often maintained at one or more contractor locations (including both prime contractors and subcontractors).
- Documentation is typically available in hard copy only. What is automated is in the source's proprietary format. When there are multiple sources, their formats are typically inconsistent. Inconsistencies in syntax and semantics dictate that documentation be delivered manually and selected portions rekeyed into the Government's databases.
- Data may become obsolete. Updates to the contractor's copy may not be passed on to the Government's copy.
- Because there is no selective access to information contained in the documentation, the Government must take delivery of a complete volume of documentation and then access it manually to find the particular item of interest.
- The time between request and receipt can be long, primarily because of the volume of data that must be retrieved, often manually.

The current information flows are depicted in Figure C-1.

The Services are responsible for establishing the structure for the information flows at each stage of a weapon program's life cycle. They maintain some data locally, requesting up-to-date component design information (e.g., layouts) and manufacturing information maintained at contractor facilities as needed. The prime contractor is generally tasked to store/maintain documentation for a weapon program and is, therefore, responsible for providing access to the support documentation produced by the program, including that of subcontractors. The subcontractors and vendors support one *or more* prime contractors in performing specific work on a weapons program; they generally maintain their own information, providing delivery to the prime contractor on request.

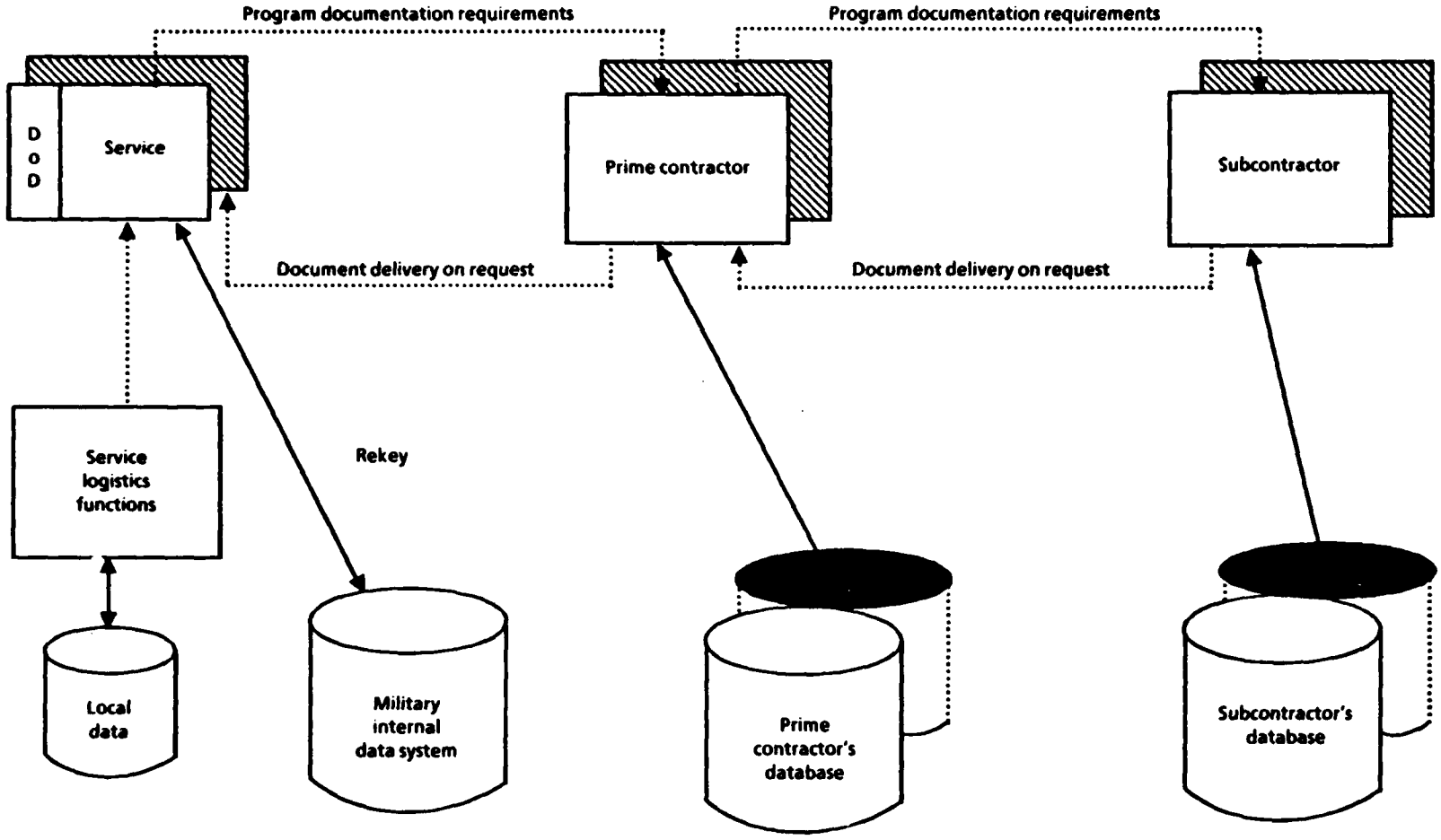


FIG. C-1. CURRENT INFORMATION FLOWS

Issues arise because each of the organizations involved

- Is autonomous, operating according to its own business rules and requirements
- Has pre-existing independent policies, hardware, and software environments
- Must maintain large existing databases of weapon systems documentation
- May be a competitor of the others, zealously guarding its own proprietary data.

The required data include conventional formatted information, text, graphics (e.g., layouts), and combinations of the three. Each type of data places different requirements on an electronic communications system. Furthermore, the same information (e.g., design constraints and physical layout), may be available in different representations and related documentation may be maintained at different locations.

2.1.2 Target Environment

What is needed is an environment in which the Government and contractors have electronic access to required information. This access will allow them to be specific about which data are needed, taking delivery of information only when necessary to support a specific function. It should not be the responsibility of the requesting organization to know where the data reside or to ensure their currency. In this environment, decisions concerning whether multiple copies should be maintained, where they should be stored, and how they should be kept updated should be based solely on cost/performance trade-offs. The environment should provide services that allow related data from multiple sources to be kept consistent and to be combined when required.

On the other hand, it may not be feasible to achieve the level of homogeneity that would seem to be needed to support this type of environment. Though the adoption of *standards* can make the environment more homogeneous, standardization alone cannot provide such an environment. There are two important reasons for this:

- Not all aspects of the environment *can* be standardized. Suitable standards (e.g., semantics for engineering data) do not exist in many cases, nor can

they be expected within the short term, particularly for technical information.

- Not all aspects *should* be standardized. Some databases may have unique requirements that need specialized facilities not provided for in the standards; conversion of large existing databases and systems may not be cost-effective; and standardization can inhibit the introduction of advanced technology. Furthermore, standardization may unjustifiably impinge on the autonomy of both source and recipient organizations, requiring major (possibly costly) changes to their computing systems and policies.

Standards are more available and more applicable at the lower International Standards Organization (ISO) layers than at the higher layers. Consequently, the target architecture will require *services* for coping with aspects of the environment that cannot easily be standardized, as well as *standards*. The information flows of the target environment are depicted in Figure C-2.

The environment supporting this data flow is complex. A single Service may have program relationships with many prime contractors. A goal is to have uniform access to documentation on *all* programs. In addition, a given prime contractor may have working relationships with more than one Service. Consistency in the requirements placed on a prime contractor by different Services and programs will reduce life-cycle costs. It may also be costly for a subcontractor to respond to different format requirements placed on it by multiple prime contractors; CALS should avoid placing costly burdens on subcontractors as well. Well chosen standards and provision of integrating services will make this easier.

2.2 Statement of the External View

The external view of the requirements is a synthesis of the functional requirements for information accessibility. It is shown in Figure C-3. The target is characterized by the following:

- Access to distributed data, according to end-user and application views, appears logically integrated. The system hides the details of data location, and the user is allowed to express all requests for information in a uniform way and to receive responses tailored to the user's specific needs (i.e., exchange of an entire file or simply an answer to a query, or perhaps support for browsing available information according to user-specified characteristics).

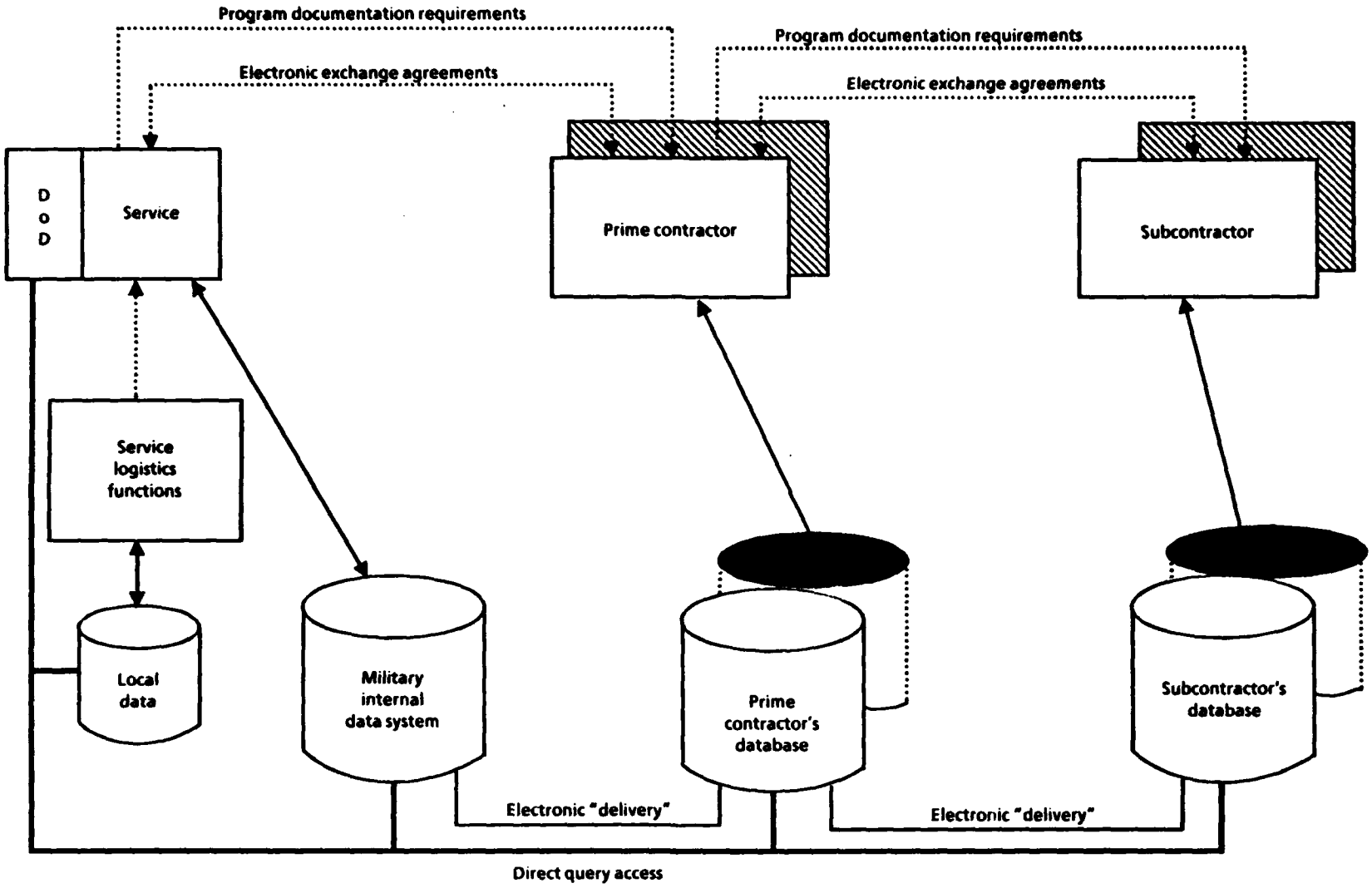


FIG. C-2. TARGET INFORMATION FLOWS

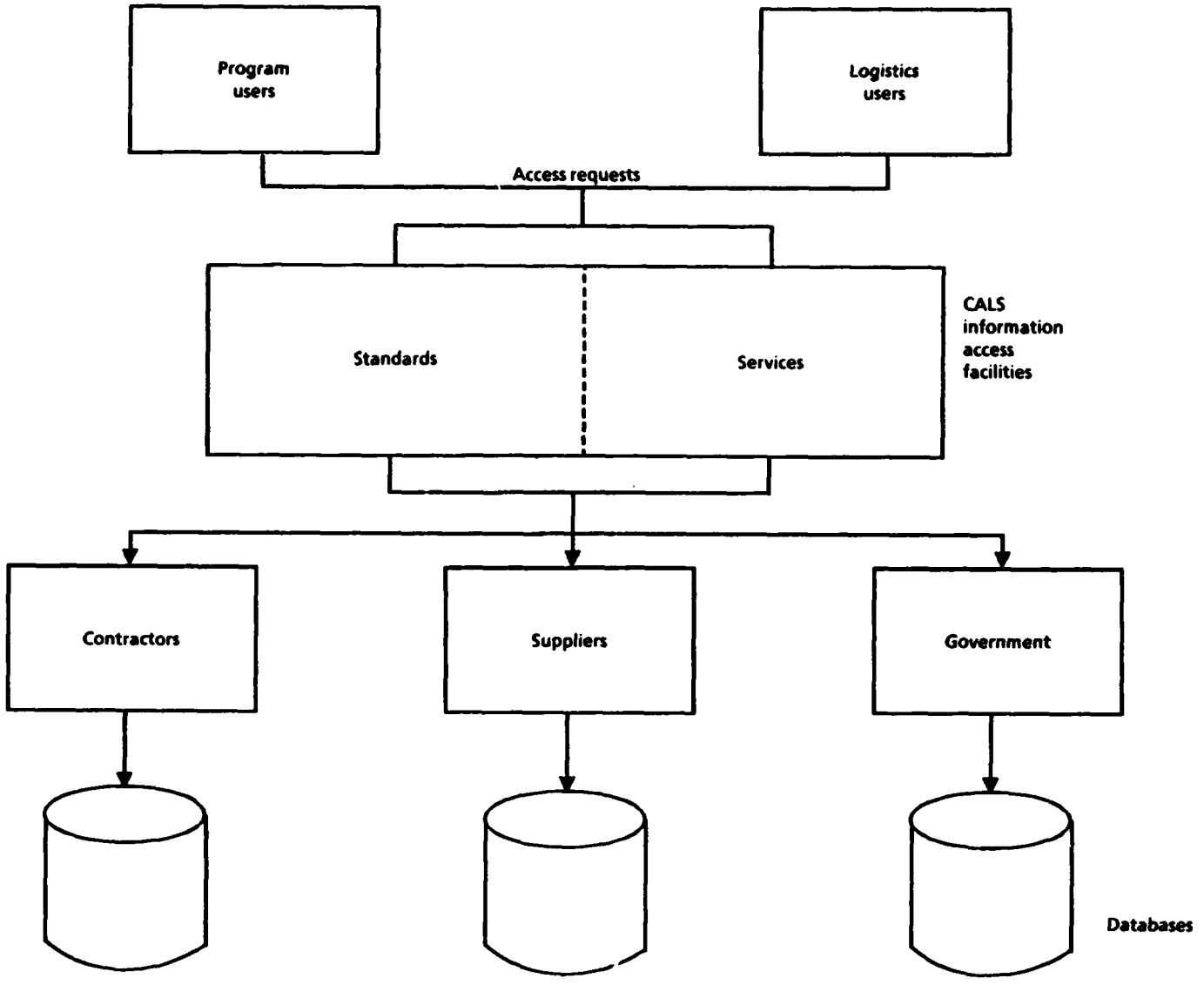


FIG. C-3. EXTERNAL VIEW OF CALS

- To the end user, it appears that access to data is direct to the source of the data. Transparent to the user, the system uses whatever path is available. This path may be direct, requiring simple mappings, or it may be quite indirect, vertically through the prime contractor and then to the source of the data located at a subcontractor. Its nature will depend in part on political considerations and in part on the physical communications paths available.

- While the long-term target is to provide completely automated support to a logically integrated information base, what the end user wants is to be able to take advantage of whatever capability is available at a given time. This means that access to data may vary depending on the capabilities available at the source node and on the communications paths to get there. The external view, therefore, is one in which the request method is uniform, but the means by which the response is satisfied varies by node and over time.

- Data are kept up-to-date by the source. This means that CALS must provide support for change control policies, versioning, and configuration management. In addition, this support needs to extend to the integrated database that the user accesses but that may, in fact, reside at heterogeneous sources. That is, while the database must be treated as an integrated whole for update purposes, updates will be triggered by the autonomous sources.

- Updates are propagated to copies of a document and to related documentation. If a user has obtained a copy of a drawing, for example, and that drawing is modified during a redesign effort, the system should recognize the association between the two events. Depending on the facilities available and on the user's needs, the system may ship the update automatically, versioning the outdated copy, or may simply notify the user that an updated version exists.

- Each site may have different needs for information, and the system supports each site according to those needs. For example, one site may wish to take delivery of all documentation at the completion of a given phase; another may wish to receive only selected component documentation (e.g., for those components most often needing repair).

These requirements imply derived requirements for how a CALS architecture should be structured -- the internal view -- which is described in the next section.

3.0 THE "INTERNAL" VIEW OF CALS DATA ACCESS REQUIREMENTS

The external requirements have implications for the functional components of the target architecture and how they should be organized. These implications give rise to an "internal" view of the requirements that identifies key technical issues regarding the approach to developing the architecture. The purpose of this section is

to provide a context for those issues, discussed in Section 4 of this appendix, by describing the components and characteristics of this internal view.

In order to meet the requirements described in the external view, CALS requires the following components and characteristics:

- Data modeling and user interface facilities for defining an integrated view of logistics information and the semantics of operations on that information. The model must be powerful enough to capture the semantics of technical information, including both textual and graphical information and combinations of the two. For example, facilities are needed to define various classes of logistics information, to specify how they are constructed from design and manufacturing data, and how operations on them (e.g., "display") should be interpreted.

- Services to provide the mappings from objects in the integrated view, requests for access to the stored underlying objects from which they are constructed, and specific access facilities that are available for the stored information.

- Specifications and standards that support communications between the sources and recipients and compatibility in form, meanings, and values of the information.

- A framework for the services, specifications, and standards that provides for interoperability among the various mapping and access services, and makes the services available to end users and applications.

- A system architecture that allows heterogeneity, is capable of being dynamically tailored to the needs of autonomous sites, takes advantage of existing components where available, and is flexible enough to accommodate advances in technology and changes in requirements.

The information access functions can be thought of as essentially "gateway" functions that, instead of linking two incompatible networks or two applications, establish links between arbitrary applications or users with requirements for access to logistics information and the range of underlying databases that contain that information. Gateways include standards that ensure compatibility between sources and recipients and services that provide needed mappings to and from the standards where compatibility cannot be ensured.

Gateway services are based on the notion of mapping functions that transform access requests specified in a uniform, integrated way into requests to specific sources. They also transform the results of these requests into integrated responses

conforming to the specific environmental requirements of the requesters. Gateways are "intelligent" in that they incorporate knowledge of the specific underlying databases and access facilities, as well as the requirements of the requesters' environments.

The internal view of the CALS target architecture is depicted in Figure C-4. It reflects the CALS role in technical data exchange as that of an IG to a distributed resource base.

3.1 Gateway Services

Gateway services map requests specified in terms of an integrated user or application view into requests to the underlying information sources. The various types of services required are described below:

- *User/application interface services* provide for the specification of requests for integrated data as well as the presentation of results. Though they are not a part of the gateway, they provide the requester with uniform access to the gateway by supporting a "global request language" embodying the semantics of the applications.
- *View management services* keep track of the objects in the integrated view, including relationships among these objects and associated operations, in order to interpret requests for operations on objects that are accessible through the gateway. They include directory services to locate the referenced objects.
- *Decomposition and routing services* map requests specified in terms of objects and operations in the integrated view into a set of specific requests aimed at the underlying databases and access services, and route the resulting queries to specific target facilities.
- *Invocation and execution control services* provide facilities for initiating and tracking requests in the distributed, heterogeneous computing environment. In performing this function they provide services similar to those of a distributed operating system. They execute the access plan produced by the decomposition and routing services and manage the submission of the individual queries and the return of responses.

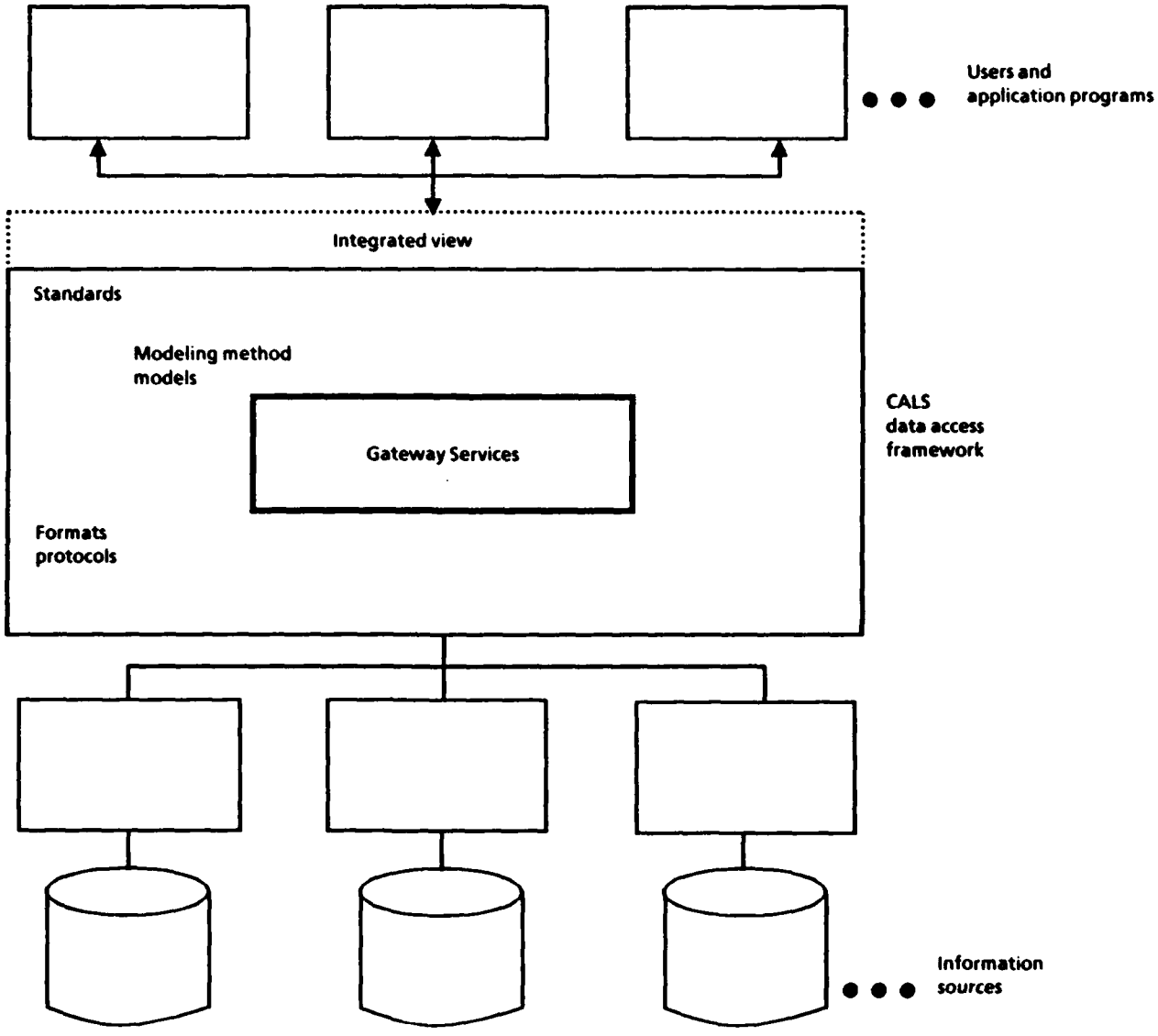


FIG. C-4. INTERNAL VIEW OF CALS DATA ACCESS REQUIREMENTS

3.2 Standards

In order to construct IGs, it is necessary to have agreements, i.e., standards (or agreed-upon specifications), covering both the syntax and semantics of the interfaces supported by the gateways. These agreements need to cover both the exterior interfaces, i.e., those with the user and/or application programs, and interior interfaces, i.e., those with the underlying services interfaced with the gateway.

Gateway services are supported by data standards and protocols for invoking services to make them accessible to requesting applications and users, for providing interoperability among the services, and for providing the ability to invoke external access services at the data sources. In addition, standards make possible extensions to accommodate new data sources.

Four categories of specifications and standards are needed to support data integration and interoperability among data access services:

- *Data formats* which provide an agreed-upon syntax for the data content of objects for communication. These provide the standard for formatting data that conform to a particular data model. Often, however, the data model is not explicitly presented, but must be derived from the formatting syntax. (This problem is a major cause of ambiguities in data exchange.)

- *Data access protocols* which provide an agreed-upon way to invoke operations on an object. The data access protocols must also embody a data modeling method describing the mechanisms of the protocol. Most current general-purpose access protocols are based on Codd's relational modeling method or on the data modeling method supported by a specific database management system (DBMS).

- *Application-specific data models* which provide a way to standardize the exterior view of the data seen by the users and application programs. These are canonical descriptions of the data that are accessible to the application (e.g., mechanical or electrical engineering).

- *Data modeling methods* which provide a way of expressing the data access protocols and the application-specific data models. The modeling method is the mechanism for documenting the semantics of the data.

4.0 ISSUES

This section identifies key issues that CALS must address in order to achieve the requirements described in Sections 2 and 3 of this appendix. These issues arise because of the problems of supporting information exchange among the Government,

contractors, and suppliers when the requesters of data have requirements, computing environments, and capabilities different from those of the sources of the data.

This discussion of issues focuses on the problems of providing access to a logically integrated database derived from distributed, heterogeneous sources. That is, it focuses on integration and interconnection issues at ISO Layers 6, 7, and above. We present the issues in five groups:

- Issues associated with making data *accessible*, i.e., with allowing end users and applications to access a distributed information base as if it were an integrated database of logistics support information
- Issues associated with *compatibility* of the underlying data sources, i.e., with how to support integrated access by combining data from heterogeneous sources in a manner transparent to the end user
- Issues associated with *control* of the information and the processes that produce or use it
- Issues associated with *transitioning* from the existing means of supporting logistics functions to the CALS long-term goal
- Issues associated with the role that *standards* play in the target architecture.

These issues emerge from two seemingly conflicting elements of the CALS goals: the need to provide users access to an integrated database and the need to derive this database from heterogeneous data sources originally developed for other purposes, in different locations, with different computing and management environments.

4.1 Data Accessibility

The issues described here concern the ability of CALS to make accessible to a variety of users, including Government agencies, contractors, and suppliers, the information needed to support logistics. Accessibility issues focus on supporting the external view of CALS requirements. They include issues associated with

- Providing a uniform *user/application interface* with the logically integrated information base
- Providing a *modeling method* that can support definition of the integrated data objects and object operations

- Logically *connecting* individual underlying databases to global access services
- Availability of *metadata*, that is, the means by which users know what data are available to them and the system knows how to map the users' views of data onto the underlying systems.

4.1.1 User/Application Interface Issues

The design of the system interface determines, in a very real sense, how "accessible" the data are. That is, the features supported by the interface will determine how easy it is to access CALS data, in terms of being able to specify what information is desired and in what format.

Also, the data request facilities can have a significant impact on performance and on lower-level data transfer issues by determining how *selective* the user can be. This latter point is particularly important for text and drawing data, since without support for selective *query* access to data, whole documents or drawings or sets of drawings must be stored locally or transmitted. Furthermore, the availability of *interactive* query or browsing facilities reduces the amount of data that must be transferred, by allowing the user to sample or preview results before committing to the transmission of large amounts of data.

Issues that arise in developing a user/application interface with distributed heterogeneous data sources include

- *Providing a request language or interface protocol that can express the data semantics of the application.* The language must support access to all data types (e.g., textual and graphics data) in a uniform way. It must allow the user to be selective in the amount of data retrieved. It must support at least that functionality to which end users were accustomed from any of the underlying data access services directly.
- *Supporting human users and applications equally well.* This point is often overlooked in interface design: end users can make use of context, scanning a document in order to infer semantic information about it; however, for the application interface, all semantic knowledge must be expressible in the request language and metadata, as discussed in Section 4.1.4 below. Trying to balance requirements for language expressiveness against requirements for uniformity is not easy.
- *Providing an interface that can be tailored to individual end user requirements, including hosting the user interface in the user's system environment.* The language must also be uniform across different terminal types (e.g., text

and graphics) while being able to exploit special workstation features as well.

4.1.2 Modeling Method Issues

The modeling method determines what data objects and operations can be defined and thus what data are accessible to the user or application. Modeling method issues include the following:

- The modeling method must support the way the user thinks about and requests particular types of data. For example, the relational model forces a user to think of data as stored in a tabular format; this modeling method is not well suited to expressing requests for engineering design descriptions or layouts. The modeling method must provide for both defining data formats and structures and for defining operations on the specified data types.

- The method must support the definition of relationships and constraints that span sources, e.g., the fact that objects from one source are "parents" of objects in a second source, or the requirement that a value must be unique across multiple databases. This, as well as requirements described later for change control procedures that span databases, requires facilities for specifying interdatabase dependencies.

- The method must also support the definition of *composite objects* whose components span sources, i.e., logical compositions of objects ("complex objects") whose components are drawn from multiple sources. The issues here concern the ability of the data modeling method and language to support the definition of such objects and the ability to specify the semantics of operations on such objects. Operations are a problem because their semantics often cannot automatically be deduced from the semantics of similar operations on atomic objects. For example, "deletion" of the composite object does not necessarily imply deletion of the components; "display" of a composite object may require special treatment of different classes of components of the object.

4.1.3 Connecting Global Access Services to Underlying Sources

These issues are concerned with defining and performing mappings from requests against the integrated view into requests to underlying sources and combining responses into an integrated result, in addition to the actual physical interconnection of the systems. Three aspects of the problem are important:

- It must be possible to define the *mappings* between the data objects in the integrated view and the underlying data from which they are derived, i.e., to describe how integrated objects are constructed. Furthermore, it must be

possible to define corresponding mappings between operations on the integrated objects and operations on the underlying data.

- Relationships between and constraints on objects in the global view must be mappable to relationships between and constraints on underlying data. This means that they must be defined using facilities of the underlying databases. This may be especially difficult if the sources use modeling methods that differ in their ability to specify relationships between data objects, or in the way in which they specify relationships, or in the built-in relationships they support.

- CALS gateway services must perform the mappings and initiate requests as needed to support global requests. Performing these functions requires not only physical interconnection but also services for initiating and tracking operations in a distributed, heterogeneous environment similar to distributed operating system services that are now beyond the state of the art.

4.1.4 Metadata

Metadata issues concern facilities for ensuring users are aware of what data are accessible to them and for describing the accessible data so that the data can be properly interpreted. The issues reflect needs of both human users and applications that use CALS data.

CALS metadata include user-readable data dictionaries, system directories that identify data locations, application-readable schemata that describe the global integrated database, schemas of the underlying heterogeneous databases, and data whose function is to "describe" other elements of the database. Management and control of metadata and providing access to metadata through CALS facilities poses several technical and management issues:

- The amount of data that need to be accessible through CALS, even for a single weapon system, is enormous. However, not all information is available or of interest to every user. Diverse user views of the data dictionary/directory must be supported.

- The dictionary/directory must provide information that not only describes what the available data are, but how they can be used, i.e., additional metadata. In addition, not all users of the data dictionary/directory are human users. Sophisticated programs need to be able to access the dictionary/directory, particularly to determine format, structures, etc., of needed data.

- Like the database, the data dictionary/directory will be a distributed, heterogeneous database. All of the issues identified in this section

associated with accessing and managing distributed data apply to the dictionary as well. Accessing distributed data through a distributed directory adds to the complexity of the integrated access problem.

- Relationships between the types of metadata, from the database-specific metadata to the metadata that describe the global system view, create a logically layered access structure. Accordingly, the facilities that manage and use the metadata must be able to support this notion.
- There is a complex relationship between metadata (e.g., a dictionary) and data. This relationship, "dictionary describes data," is not static, and change control procedures for the dictionary must reflect the current status of the data it describes.

4.2 Data Compatibility Issues

Data compatibility issues include three classes of possible incompatibilities: syntactic differences, which affect the form of the data; semantic differences, which affect the meaning of the data; and problems of overlapping sources, which may result in conflicting data values.

4.2.1 Syntactic Issues

Syntactic issues arise because of differences in *representation* of the various types of data. CALS requires exchange of technical and associated management data. Technical data include conventional formatted data (such as are supported by ordinary DBMSs), textual, graphical/drawing data, and combinations. Associated with each type of data are differences in format [e.g., American Standard Code for Information Interchange (ASCII), Extended Binary Coded Decimal Interchange Code (EBCDIC)] or representation (units, scale, and encoding).

Syntactic issues also include representation of various data *structures*. Such differences occur when data are defined using different data models, when components of the same model are used in different ways, or when different types of systems are used to store the data. For example, different systems may model the same data by fields in a record, rows in a table, cells in a matrix, nodes in a graph, or lines in a drawing.

Often, syntactic issues can be resolved by the existence of standards, even though multiple standards may have to be accommodated. In general, representation differences are often resolved through simple arithmetic transformations or table look-ups. Structural differences are often reconciled through mappings from one data

model to another or by mapping requests against one structure into requests against another. However, the mappings may be quite complex, they may not be unique, and some may be far more efficient than others.

4.2.2 Semantic Issues

Semantic issues affect a recipient's ability to interpret the transmitted data. They include differences in names, representation of relationships, and meanings of objects in the database.

- *Naming discrepancies* include differences in how an object is uniquely identified, differences in naming conventions, and use of different names for the same objects or their attributes (or use of the same name for different objects).
- Issues associated with the *modeling of relationships* include how relationships are represented (e.g., relationships between data elements might be represented by common values or by pointers) and what relationships can be represented or have built-in operations to support them (e.g., TYPE-OF, COMPONENT-OF, VERSION-OF).
- Issues concerned with a common *understanding* of application-specific elements includes not only the meanings of objects in the application but exactly what those objects are. Applications may have to be in agreement as to what a "wire" is, what are the names of its properties, and what are the relationships of those properties. Furthermore, applications need to agree on the terminology and concepts to support common activities. The issue may not be just a difference of opinion on what are the properties of a "wire"; one application may know "wires" and the other may not.

Semantic differences can be difficult to resolve because they may depend on the database designer's *intent* or *understanding* of the data. This intent or understanding may have to be provided through explicit instructions for resolving each type of conflict. The few available standards typically define semantics vaguely, incompletely, and not in a fashion that would allow them to be derived automatically. In the long term, the issues will be compounded because of the need to describe not only objects such as parts, drawings, etc., but also processes such as tests to be performed, conditions to be tested, etc.

4.2.3 Overlapping Sources

Discrepancies that arise from overlapping sources include conflicting values and constraints. They are often resolved by specifying non-overlapping conditions for selecting from each source.

- For data with conflicting values, the requester must be made aware of the possibility of such conflicts so that he or she can specify a "preferred" source. Preferences can be stated in terms of conditions under which each source is to be used.

- Differences in constraints on replicated or partially replicated data from different sources are a more complex problem for several reasons. First, it may not be possible to detect conflicts between the specified constraints even though conflicts are inferred by the constraints. Second, multiple ways of reconciling such differences are possible, so they cannot be reconciled automatically (for example, one might take the union of all constraints, or one might select the more restrictive of constraints, or drop conflicting constraints). Finally, mapping constraints specified on one database structure or format into constraints on different structures or formats may be extremely difficult.

4.3 Data Control Issues

Control issues concern problems of ensuring the reliability of information while preserving the autonomy of the information sources. They arise mainly in the context of maintaining or updating data in a distributed, heterogeneous environment. Difficulties arise because the users of the information are often not the sources of updates, nor are they *responsible* for maintaining the information.

Issues associated with data control include the following:

- Ensuring data *timeliness* and *accuracy*. Ensuring timeliness and accuracy are difficult problems even in single-site, homogeneous systems. They are far more difficult where data are maintained outside of the sources, where local control for maintenance of the data resides. However, there are benefits to some data replication, including reducing retransmission of frequently used data and increased reliability. In these cases, CALS must provide facilities for ensuring a user request obtains the appropriate version of the data.

  Maintaining multiple copies may be accomplished by reflecting updates directly in all remote copies (a process that requires dealing with network partitions and with differences in data representation among systems); alternatively, it may be accomplished by keeping track of changes to the

source copy, notifying users of remote copies only when they attempt to access that copy (which requires the ability to detect an attempted access). Additional problems include how to define "source" copy, how to control updates that originate at remote locations, defining who can update, and how updates are propagated. In general, one of the benefits of CALS will be to reduce data redundancies through increased global access capabilities.

- Providing for data *integrity* in a distributed, heterogeneous environment. Facilities for ensuring database integrity include checkpoint, backup, and recovery facilities. However, in a heterogeneous environment, the ability of the system as a whole to perform these functions depends on the facilities available in the underlying systems. This issue is difficult to resolve except with "cooperating" systems, because (1) some of the underlying systems may not have the required backup and recovery capabilities; (2) the capabilities may not be consistent across systems; and (3) it may not be possible to control invocation of the underlying facilities in a manner consistent with a concept of "global transaction management."

- Specifying and testing *constraints*. In the general case, database updates are first tested against constraints specified in the metadata that govern the consistency of the database. Similarly, it must be possible to specify cross-database constraints for testing updates to the integrated, heterogeneous database. Difficulties include specifying how constraints on the global database are to be mapped into constraints on local databases, detecting failure of a local constraint, and handling exceptions when a local constraint fails. Support for global transaction management, identified above, is critical to ensuring consistency of the integrated database.

  Even capturing constraints is a problem. Currently, most constraints are enforced by the applications, external to the DBMS. These constraints may be expressible only in terms of *programs* that evaluate them. In order to integrate such constraints with the global view of the database, they must be describable in the data model and invoked by the global services.

- Implementing *change control* procedures. There is a need for management procedures that implement change control where a change to one object triggers changes to related objects, especially where distributed, heterogeneous databases are concerned. These procedures include versioning and configuration management. The fact that the objects are distributed is, of course, an additional problem.

- Enforcing *security*. Some organizations may wish to restrict access to data and metadata, and the system must be able to ensure global system security by respecting and enforcing the access restrictions of the underlying systems. These access restrictions may include allowing only certain classes of users to access certain classes of data, or they may restrict the types of data aggregation allowed, and they may differ for each system. Support for

browsing and providing access to the dictionary both introduce additional security problems.

4.4 Transitioning Issues

The CALS transition plan must address the feasibility and cost of transitioning from operating in the current environment to realizing the long-term goals stated in Sections 2 and 3 of this appendix. Issues that must be addressed include

- Dealing with *existing data/systems*. The time required for CALS transitioning is long and costly because of the need to convert existing weapon system documentation. CALS must be able to support integrated access to *existing* data/systems, which includes all of the aspects that were discussed earlier in this section. The transition plan must address the implications of this requirement in the short term and throughout the CALS life cycle.

- Use of *source data access tools*. In order to preserve local autonomy, or when it is not cost-effective to standardize source databases, it may be desirable to use tools local to the source to provide data access services. However, local tools may have incompatibilities and missing features. Tools that provide the access services may support only limited or unusual commands. In addition, the tools may lack needed access capabilities, particularly capabilities required for combining partial results (e.g., joining data, aggregating data, transforming values, and sorting).

- *Integrating data access services* requires generating a strategy that will perform reasonably, if not optimally. This is difficult where the same operation may have vastly different costs in different source systems. The same operation may not be available for different systems, and the operations that are available may be very difficult to compare in terms of cost.

- *Changes* in requirements and *advances* in technology. The transition plan cannot assume that the long-term goal is static, but must instead address CALS life-cycle issues. The degree to which the system is extensible to accommodate new requirements and to embrace advances in technology will determine its success. It must be able to embrace new technology both in the underlying systems and in integration technology. It must be able to provide access to new kinds of data and must be able to provide the data in support of new uses.

- *Tailoring*. As discussed in Sections 2 and 3 of this appendix, preserving local autonomy is a legal and management issue critical to the success of CALS. To resolve this issue, the transition plan must clearly specify how organization-specific policies, technology, tools, and requirements will be accommodated by the CALS architecture. While all participating organizations are likely to benefit from adopting CALS standards, different

organizations will have systems at different stages of transition. Also, organizations will want to be able to take advantage of local technological advances. CALS must also be able to support the concept of local extensions to CALS standards.

4.5 Standards Issues

The role of standards in realizing the CALS target architecture must be clearly identified. Selection and adoption of standards will be difficult for the following reasons:

- The process of developing a formal standard is a lengthy one: 4 to 7 years, depending upon complexity. The review cycle for American National Standards Institute (ANSI) standards is 5 years. Contracts and weapon system developments cannot be held up while standards are developed. In addition, weapon system development must have access to the best available technology, even when that technology is not reflected in a standard.

- The mere adoption of a "neutral" data format cannot alone achieve a homogeneous system. Defining a single neutral format suitable for all data in the system is extremely difficult. (In fact, none has been produced successfully, thus far, even in environments much less demanding than CALS.) Moreover, given the extended lifetime of CALS, such a neutral format would have to encompass future data types that are presently unknown, in addition to the data associated with current engineering technology.

- Given the long projected lifetime for CALS data (10 to 20 years), it will not be possible to hold standards constant for the life cycle of a single weapon system, much less for multiple weapon systems. Considering the large volume of data to be maintained, it is unlikely that the Government will be willing to bear the cost of periodically converting all the data from old versions of standards to newer versions.

In particular, the transition plan must address how to accommodate overlapping standards in certain areas (e.g., organization-specific standards), and how to succeed in the face of missing standards in others (especially at ISO Layers 6 and 7), in view of the long leadtime for adopting standards. The plan must also address how to accommodate changes over time, and how to ensure all standards are extensible to accommodate evolving requirements.

5.0 APPROACHES TO PROVIDING CALS DATA ACCESS FACILITIES: A TARGET ARCHITECTURE

This section describes approaches to developing CALS data access facilities within an appropriate architecture. Four approaches are important to providing data access and integration of logistics information for CALS:

- Standards
- Logical integration
- Framework
- Object orientation.

These approaches are not independent but are in fact complementary.

5.1 Standards

In this section we discuss the role of standards in the overall CALS IG architecture. Appendix E includes a survey of current relevant standards development efforts.

Standards establish interface agreements among CALS users, the weapon system contractors supplying CALS data, and the developers of IGs for the CALS system. They allow users to know what to expect of the system in terms of standard data representations and application-specific data models. They also help reduce the cost of IG development by limiting the number of interfaces that must be supported. Use of generally accepted industry standards will increase the likelihood that the underlying systems and tools (e.g., workstations, DBMSs, etc.) will provide compatible interfaces, thus avoiding the need for special-purpose software to support the required interfaces. Furthermore, standard application-specific data models will provide technical guidance for agreements between the Government and weapon system contractors regarding data deliverables.

Although standards will play an important role in the CALS architecture, not all interfaces can or should be standardized. Nor should those that *are* standardized necessarily be limited to a single standard. Because of the issues raised in Section 4 of this appendix, it is unlikely that CALS can rely on the selection and enforcement of a single standard (or a single set of standards) as the basis for IG capabilities.

Instead, CALS must be compatible with multiple standards, not just a single standard for each class of data or interface.

CALS will need standard data modeling methods. The standard data access protocols used will normally be determined from these modeling methods. Similarly, application-specific data models will be expressed using the data modeling methods, and data exchange formats will be derived from the application-specific data models by providing an explicit syntax for formatting the data described by the model.

In the near term, however, it is likely that the order of derivation just described will be reversed, since data formatting standards and data access protocols are much more common today than are standard data modeling methods powerful enough to express the semantics of engineering data. In the long term, on the other hand, as the requirements for data modeling methods for engineering data are better understood, these standards will be derived in the described sequence.

5.2 Logical Integration

The goal of providing access to an integrated database without impinging on local autonomy and the need for a low-risk implementation and transition both have implications for the approach to a target architecture and for its development. One approach to providing integrated access to data derived from heterogeneous sources is to provide the "illusion" of integration without actually forcing the underlying databases and services to conform to the standards for integrated data, i.e., to provide logical, but not physical, integration. This approach can have several advantages:

- It can support specialized data and systems difficult to coerce into the standard.
- It can alleviate the need to convert very large existing databases.
- It avoids impinging on local autonomy.
- It is easily extensible to incorporate new data types and systems.

The objective of such an approach is not to avoid standardization, but rather to provide integrating services where standardization is infeasible or not cost-effective. The function of these services is, essentially, to hide the heterogeneity of how data objects are stored and how access operations are implemented, i.e., to provide location and access mechanism transparency.

The services that are required in order to provide such transparency include

- *Mapping and translation services* which translate from a global model and language into the specific data models and data access languages of the underlying databases and facilities. Such services formulate each routed request into a query or command that can be understood by the target system. Mapping services map from the data model of the global request language to the data model of the target system, essentially expressing the needed semantics from the global model in the semantics of the target system model. The translation services translate from the global language syntax to the syntax of the target data access tool.

- *Composition and reconciliation services* which form a single, integrated response from the individual results of the requests to the underlying databases and access services, possibly conflicting. These services involve more than simply combining the data; they may also have to resolve inconsistencies between conflicting data values (e.g., by selecting from a "preferred" source) or respond to the problem of missing or incomplete data.

Additional services may be needed to make up for facilities missing from the underlying facilities, rather than merely providing "integrating services." Depending on the application and on the end-user view of request capabilities, there may be a need for query support that is simply not available from the underlying systems. Access to these services can be provided through the gateway in the same way that access is provided to the underlying resources, but CALS will need to develop the services.

For example, if end users have defined an object that is a part or document hierarchy that they want to be able to query, *recursion algorithms* may be needed to traverse the hierarchy relationships in order to support the queries. If the data management services containing the supporting data do not provide for recursion, such facilities could be provided by CALS. This approach allows an organization to meet short-term data access and query requirements and is easily replaced when the organization upgrades underlying data management facilities with state-of-the-art DBMSs. In this case, the gateway simply revises (in a way transparent to the end user) the means of satisfying the same request using the underlying facilities.

5.3 CALS Framework

It follows from the discussion in preceding sections that CALS should provide the *means for integrating* the existing environment rather than being a single *integrating system*. This approach gives rise to the concept of a *framework* that

focuses on the interoperability of existing or planned systems with CALS-provided integrating services. Such an approach provides the means by which two seemingly contradictory CALS goals can be reconciled: providing *integrated* access to data from heterogeneous sources while preserving some degree of *autonomy* of those sources. It also supports the notion of an extensible CALS tailorable to sites with different databases and computing environments and varying levels of implementation of CALS services and standards.

The framework must link together two types of components: services that provide data access and integration, and specifications and standards that allow interoperability among the services and between the gateway services and the underlying resources. The framework determines how gateway services interoperate and the relationships among them, as well as the relationships between particular services and associated specifications and standards. In addition, the framework determines how gateway services can be provided in a manner consistent with the goals of noninterference with the underlying databases and environments, and in the context of extensible, replaceable components.

Although gateways are often depicted as a layer of services between a user request and the target data access services, it may be useful in designing and constructing gateways to view them as a cooperating network of services – not as a fixed hierarchy of interrelated layers.

The framework's structure should ensure services intervene in the request path only to the extent necessary to route a user request to the appropriate underlying data access service(s). This arrangement not only provides a more flexible structure but may, in fact, avoid the heavy processing overhead typical of deeply layered systems. For example, the gateway should recognize a request already expressed in terms of the underlying system (e.g., a direct request for a file transfer) and should pass that request directly to the target operating system. In this example, the gateway need act only as a traffic cop, invoking services to locate the target object and directing the request to the underlying resources that can handle it.

To support more complex requests, additional gateway services must be invoked. For example, a query regarding the documentation of an assembly and some of its components might need to be *decomposed* into separate retrieval requests and routed to different underlying databases. The requests would then need to be

mapped into concepts supported by the data models of the target systems and translated into their query languages. Then the individual results would need to be *combined* to produce a single answer to the original query.

The framework definition should focus on the interfaces with and interoperation of these gateway services. By defining the component functionality in terms of interfaces, CALS developers can ensure the architecture does not dictate an implementation approach to the facilities provided by each component. This approach to key architectural characteristics means that each component is replaceable, thus ensuring extensibility of the target architecture.

The approach provides two benefits. First, it ensures one can pick and choose from the latest research and prototype results in key areas, such as information modeling, query decomposition, and dictionary management. Second, it is a description-driven approach to architecture development that makes it easy to replace a component in order to take advantage of technological advances as they occur or in order to respond to evolving requirements. It extends the concept of extensibility in the underlying services (a key characteristic of the "framework" approach) to extensibility in the framework itself.

The services can interoperate within the framework only because they rely on the specifications and standards describing the externals or interfaces of the data and operations. Note that we group together specifications and standards, where both must be external to the implementation and both must support interoperability. We use the term "standards" merely to indicate specifications that are adopted more widely than just within the organizations served by a gateway. Wide recognition and adoption of standards limits the variations that must be supported by the various gateway services.

5.4 Object Orientation

The requirements and issues that CALS must address lead us to believe that an *object-oriented* approach will benefit the *structure* of the CALS framework, as well as the *implementation* of the services. We use the term "object oriented" in its broadest sense, to indicate a way of modeling problems and an approach to providing services, rather than as describing a specific type of programming language.

Most object-oriented systems, object models, and object-oriented approaches in general support the following concepts:

- *Object identity.* The concept of "objects" independent of their properties or operations, or construction from lower-level data. This concept provides a means for the user or application developer to specify requests on objects in his or her mental image of the application. For example, the user can define operations on objects such as "wing design" or "schedule," rather than needing to map a request to one on "relations" or "records." Most object models support the definition of "complex objects" (objects composed of other objects), and operations on them as well. This approach will provide a means for defining logistics data objects in terms of design or manufacturing data from which they are derived.

- *Abstraction.* The separation of the externals (the exposed part or interface) from the internals (the hidden part or implementation) of objects and operations. This separation provides the basis for hiding the heterogeneity of the underlying databases and tools. In object-oriented systems, the interfaces are clearly defined and unchangeable, whereas the way in which data objects are stored or operations are implemented is hidden and can be replaced with better, faster, etc., versions, thus supporting the needed extensibility for CALS.

- *Encapsulation of objects and operations.* The grouping of objects into "types" based on common properties and operations, and the linking of operations to specific types of objects on which they operate. This grouping provides control over the operations, allowing only appropriate access operations for each type of object, e.g., "versioned" object or "textual" object. In addition, most object models support the definition of operations with the same name but different, type-specific implementations (polymorphism); for example, "display" text and "display" drawing could be defined with appropriate implementations for each object type. Following this approach will facilitate the development of user interfaces that can be uniform across data types and adaptable to different terminal environments. In addition, it will provide useful control for change operations in the distributed environment.

- *Operation invocation.* A uniform way of invoking all operations, independent of the type of operation involved and the numbers and types of their operands. This feature makes implementation easier and often makes possible powerful user interfaces by hiding heterogeneity among operations and object types.

We do not contend that such an approach offers more than the obvious benefits or that it is a cure-all for difficult issues. We do contend that, as a general approach, object orientation provides specific benefits addressing the CALS requirements. This

is not to say that other approaches could not work, or that an object-oriented programming language is required for implementing CALS.

APPENDIX D

COMMERCIAL AND EXPERIMENTAL INTELLIGENT GATEWAYS

CONTENTS

		Page
1.0	Basic Gateway Systems	D- 3
1.1	Technical Information System (Lawrence Livermore National Laboratory)	D- 3
1.2	Knowledge Gateway Service (Telebase Systems)	D- 4
1.3	IRVING Library Network (Minicomputer Systems, Inc.)	D- 5
1.4	Chemical Substances Information Network (Computer Corporation of America)	D- 7
2.0	Expert Front-End Systems	D- 8
2.1	Connector for Network Information Transfer Massachusetts Institute of Technology	D- 8
2.2	Front End for Database (General Telephone and Electronic Laboratories, Inc.)	D-10

COMMERCIAL AND EXPERIMENTAL INTELLIGENT GATEWAYS

This appendix concentrates on the user interface capabilities provided by the basic gateway systems and the expert front-end systems discussed in Section 3 of the main text. The approaches presented here use a minicomputer or microprocessor as a front end to perform various functions for communicating with remote systems. Software of varying levels of complexity have been written to support these systems.

Each approach was examined from a conceptual viewpoint. We did not test hardware or software to determine whether they met vendors' specifications and claims, nor did we conduct a detailed examination of manuals describing implementation of hardware and software in the various approaches.

1.0 BASIC GATEWAY SYSTEMS

Four basic intelligent gateway (IG) systems in various stages of development and use are discussed briefly below. These systems provide user-friendly access to various types of bibliographic information, both commercial and Federal, and are included as examples of past successful gateway efforts.

1.1 Technical Information System (Lawrence Livermore National Laboratory)

Since 1975, Lawrence Livermore National Laboratory (LLNL) has been developing the Technical Information System (TIS) which provides automated connections to information centers in the United States and overseas. TIS gives authorized users access to more than 30 geographically distributed systems and computers, including large Federal and commercial bibliographic information centers and various numerical data evaluation centers. TIS permits immediate access to and use of these data centers via a single access to an IG.

TIS is accessible over the Federal Telecommunications System (FTS), commercial telephone lines, the Wide Area Telecommunications Service (WATS), the (Defense) Advanced Research Projects Agency Network (ARPANET), and the Tymshare Corporation Network (Tymnet). TIS leads the user to available information resources by means of a master directory and automated access

procedures. Communications are established automatically, with redundant communications paths to the destination database. The user selects the name of the desired resource from a menu. Users are granted selective access to external resources on a need-to-use basis.

The TIS gateway, which operates in an asynchronous terminal environment, selects the optimum communications pathway, translates protocols through external protocol emulators, provides the host-to-host dialog, translates files, and offers subsequent postprocessing. TIS also provides overall transaction control, accounting, and security. Interactions with users are menu-driven and self-guided, and on-line help for several levels of expertise is offered. The user must be familiar with the selected resource, since search negotiation must proceed according to the syntax and logic of the target system. Extracted information can be placed in topical data files on TIS for subsequent postprocessing, analysis, and graphical display.

1.2 Knowledge Gateway Service (Telebase Systems)

Telebase Systems has introduced an electronic information-retrieval service termed the Knowledge Gateway Service and commercially known as EasyNet. Telebase developed the EasyNet service in 1984 under sponsorship of the National Federation of Abstracting and Information Services (NFAIS), the official trade association of database producers. The service provides access to more than 920 databases through 12 vendors. Additional systems have been developed for use limited to the sponsor organization. In all, 17 unique gateway systems have been developed by Telebase Systems.

Designed for nonexperts, EasyNet requires neither specialized training nor learning a new set of retrieval commands. Untrained users can obtain information from a broad range of databases without having to learn multiple log-on procedures and search languages. However, users generally develop their own downloading and postprocessing routines. For inexperienced users, EasyNet automatically identifies the database containing the topical information the user needs. After EasyNet leads the user through a series of menu screens, it recommends a database or lists eight possible databases. It automatically translates "English-like" questions into the appropriate query formats to search specific databases. The system then automatically dials the proper database vendor, logs on, accesses a database, and initiates

a search. The user need not know the command language of the remote system nor learn a common query language.

Advanced users have the option of directly selecting any of the individual databases offered through EasyNet. Even for those who know which database they want to scan, the system's common-language translation system can be helpful. Knowing what database to use is often still several awkward steps away from actually getting to the data. Various access vendors have their own intricate search languages. EasyNet services keep up with the changes made to both the databases and the vendors' retrieval systems. A help mode for system problems is also provided, permitting users to talk to operators familiar with the databases.

1.3 IRVING Library Network (Minicomputer Systems, Inc.)

IRVING is a consortium of public libraries (Aurora, Boulder, Denver, and Jefferson County) in Colorado. The consortium is attempting to connect disparate computer systems in an on-line, interactive mode using a proposed common network language. Because of the industry-wide implications of interfacing heterogeneous computer systems and the portability of the network software, much interest has been generated by this effort.

Formed in 1978, IRVING issued a joint request for proposals in 1979 to purchase common automated systems. Vendor responses and low-bid requirements split the market and resulted in the installation of dissimilar turnkey systems at each library (two systems with Tandem Computers equipment; one system using Digital Equipment Corporation hardware; and one using a Sperry minicomputer). The design for connecting these systems was based on the then-emerging international model for Open Systems Interconnection (OSI) and is compatible with similar computer-to-computer communications protocols being developed by the Linked Systems Project sponsored by the Council on Library Resources at the national level. Figure D-1 shows the architecture of IRVING as of August 1986.

The IRVING design uses front-end processors to network library host computers to form a system of distributed information utilities that may be accessed on site or by dial-up terminals. The library network software provide mutual access to member library databases, handles network requests, and manages network circulation.

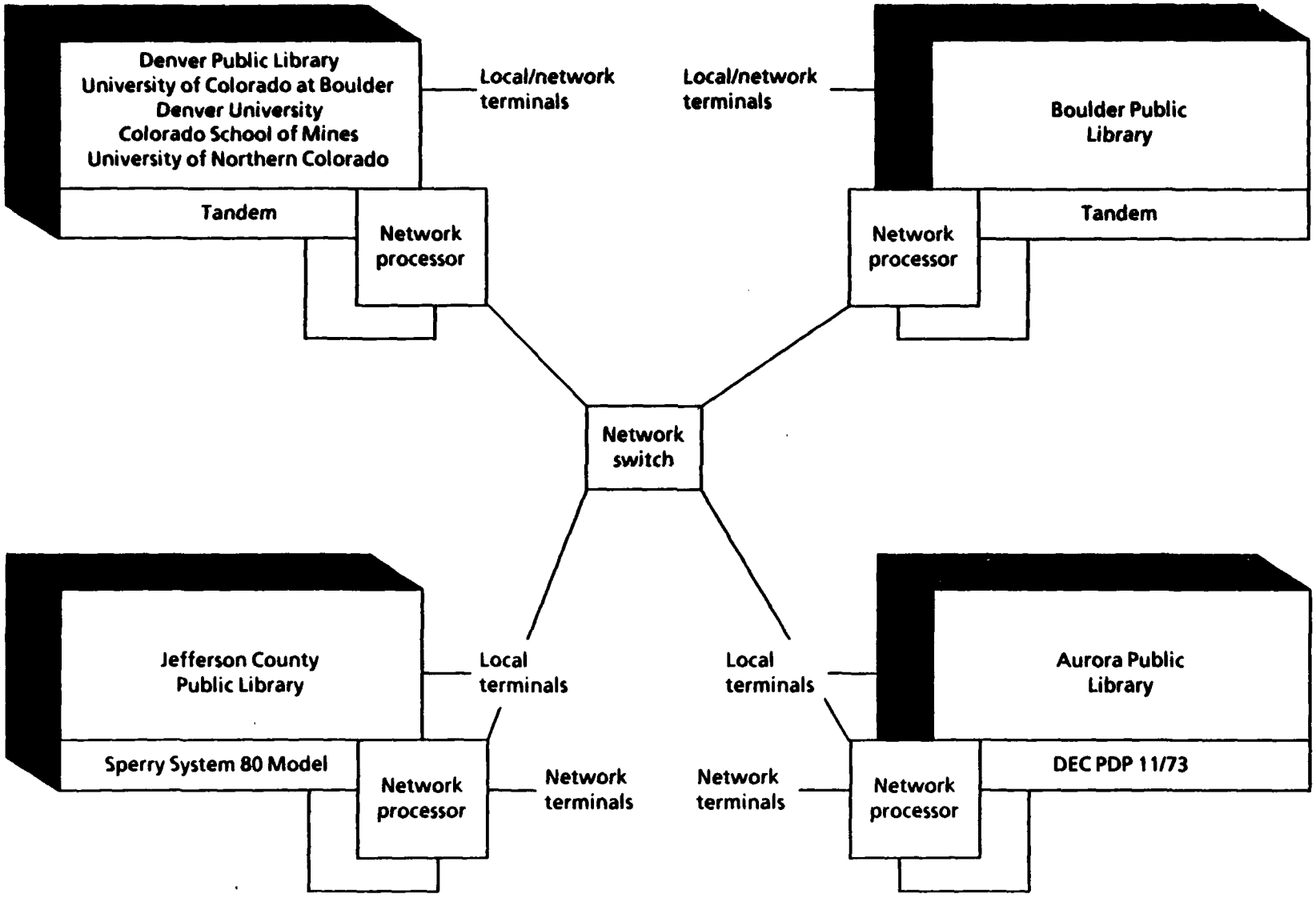


FIG. D-1. THE IRVING NETWORK

1.4 Chemical Substances Information Network (Computer Corporation of America)

The purpose of the Chemical Substances Information Network (CSIN), a coordinated network of on-line chemical information systems, is to satisfy information requirements associated with the Toxic Substances Control Act and related legislation. The network was designed to serve Federal, state, and local Government agencies with regulatory or research responsibilities, as well as scientists, industry, educators, public interest groups, and others. CSIN provides a communications network that links many widely dispersed, independently operated, heterogeneous information systems containing data on nomenclature, composition, structure, properties, health and environmental effects, production, uses, regulation, and other aspects of chemical substances. While preserving the integrity of the information resources, CSIN facilitates their joint use without requiring that the user know how to search each resource individually.

The first version of CSIN was completed in December 1979. It provided facilities for

- Connecting to each of four remote information systems
- Capturing data received from these systems
- Transforming the captured data or stored lists of query terms to a format suitable for searching one of the remote systems
- Substituting transformed data for keyboard input
- Editing and manipulating the files of stored information.

The second version of CSIN includes the functions of the first plus the addition of a query script facility. This facility enables most users to perform routine CSIN transactions by invoking predefined script that handles all interactions with other systems, retrieves output from them, and presents output to the user's terminals. Query scripts are written by CSIN information specialists and made available to the user community. Since the script hides the details needed to carry out the transaction, users who have little training can run complex multisystem transactions.

2.0 EXPERT FRONT-END SYSTEMS

Two efforts discussed here address the need for effective search strategy formulation through the application of artificial intelligence technology and the development of specialized expert systems. Both efforts are in the prototype development stage.

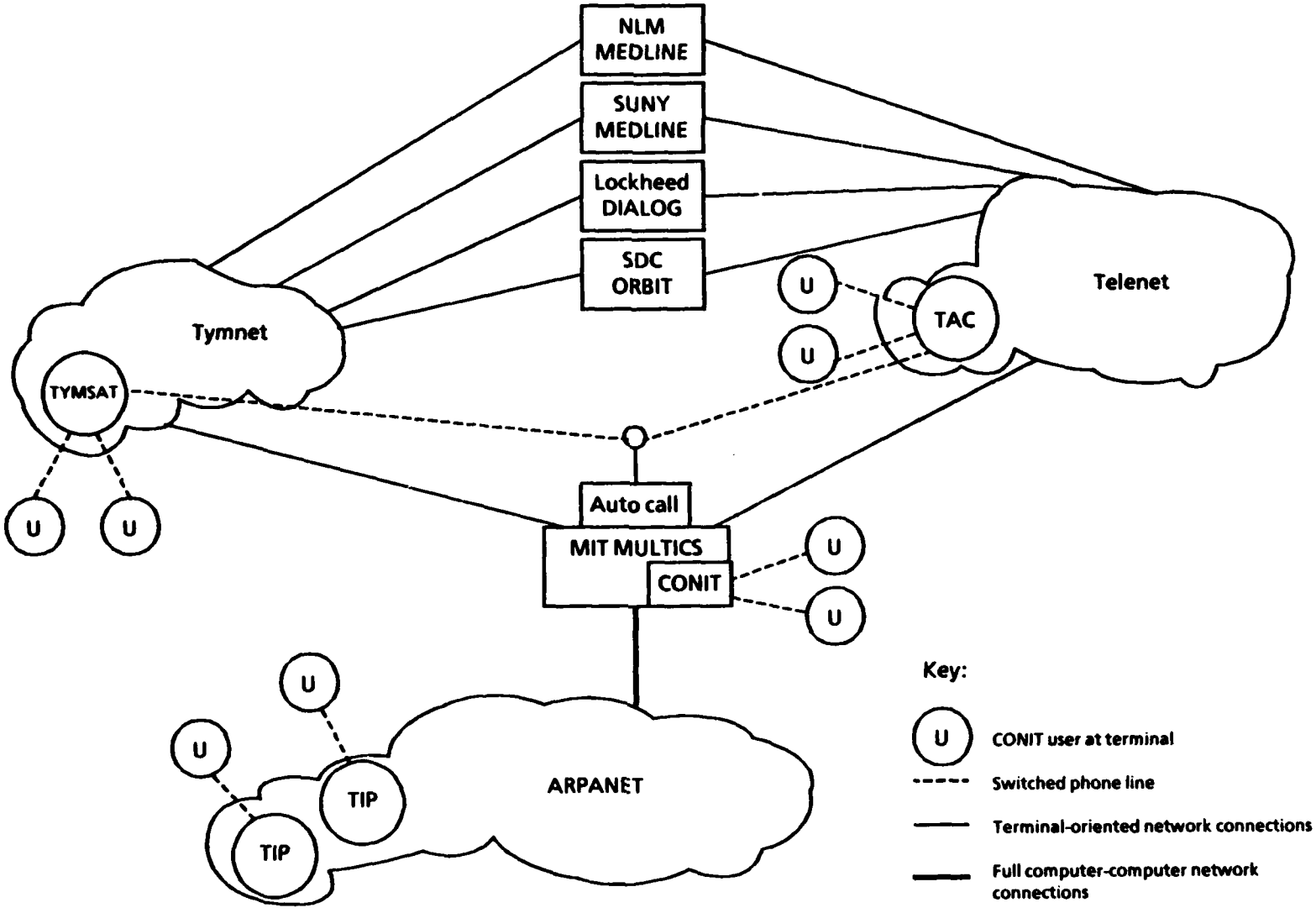
2.1 Connector for Networked Information Transfer (Massachusetts Institute of Technology)

Connector for Networked Information Transfer (CONIT) is an experimental front-end system implemented on the Massachusetts Institute of Technology (MIT) MULTICS computer system. MULTICS has connections to ARPANET, the General Telephone and Electronics (GTE) Laboratories, Inc., Telecommunications Network (Telenet), and Tymnet. These network connections make it convenient for users at remote terminals throughout the United States and in many foreign countries to access MULTICS.

Three major retrieval systems are part of the CONIT network: Lockheed DIALOG, Systems Development Corporation (SDC)'s ORBIT, and the National Library of Medicine (NLM) MEDLINE system, which is implemented in slightly variant forms at two locations – NLM in Bethesda, Maryland, and the State University of New York (SUNY) in Albany, New York. The two MEDLINE systems are essentially identical in structure but have different databases and network connection protocols. The ORBIT and MEDLINE systems have basically the same command language, but important differences exist in a few functional areas. DIALOG represents a system with a very different command language and a set of retrieval functions that differ in several major respects. The interconnections of CONIT with the various networks and retrieval systems are shown in Figure D-2.

Some of the features and techniques of CONIT include

- A simple, easy-to-use common command language (CCL) leading to a translating, virtual-system approach to a network of heterogeneous systems and databases
- Extensive, dynamic computer-aided instruction (CAI) for teaching use of the CCL and the development and modification of search strategies



Note: TAC, TIP, TYMSAT: network communications processors.

FIG. D-2. MIT'S CONIT EXPERIMENTAL NETWORK

- Selection of only the most important retrieval functions to include in the CCL and only the most important core of those to recommend to the users initially
- The automatic handling of certain procedures such as log-in protocols, search overflow conditions, and search regeneration and repetition in multiple databases
- An automated Boolean, all-fields, content-word-stem search operation based on a user's free-vocabulary topic phrase description.

The CONIT system holds potential for further sophistication. To date, it has no well-established optimal search strategy; much of what a human intermediary does is intuitive or trial-and-error. One goal of the continuing CONIT effort is to determine what approaches are most effective and to develop ways to implement them on the computer using the techniques of expert systems. This effort could lead to development of an "intelligent" interactive system that researchers can use to query the growing network of databases directly. However, it is important to recognize that CONIT's current form of implementation is highly experimental. The prototype, operational since 1976, has undergone a series of enhancements over the years. The focus is on providing a continuing experimental environment rather than a production-based one.

2.2 Front End for Databases (General Telephone and Electronic Laboratories, Inc.)

GTE's front end is called an Intelligent Database Assistant (IDA). Distinct from the issues of traditional database management systems (DBMSs) such as efficient data storage and optimal search strategies, the major issues in IDA design are

- Natural language dialog-based user interfaces for querying multiple databases
- Expert systems for automatic database selection and query planning
- Portable access to multiple databases across different DBMSs.

The Front End for Databases (FRED) system, developed at GTE Laboratories, is an example of an IDA. FRED has been applied to textual medical databases and to a relational personnel database. The system accepts queries specified in English or by menu, clarifies them if necessary, selects the proper database, and generates the

appropriate database query. FRED is a hardware/software layer that can be interposed between users and database systems. User queries and commands are routed to FRED, which sets up appropriate database connections and makes necessary language translations so that different databases all have uniform appearance to the user. The user/FRED dialog is conducted in natural language (English). Since one language is used for all databases, use of the system requires minimum initial orientation.

The FRED user language combines positional techniques (e.g., menus) and English natural language in a highly interactive system that can be used with simple communications terminals. Instead of attempting to develop a complex natural-language system that would permit users to submit increasingly abstruse queries, the combined approach uses interactive feedback from the computer (positional prompts and cooperative responses) to help users formulate more effective natural-language queries.

APPENDIX E

SURVEY OF RELEVANT STANDARDS DEVELOPMENT EFFORTS

CONTENTS

		Page
1.0	Data Formats	E-3
1.1	Facsimile Transmission Standards	E-3
1.2	Graphics Standards	E-3
1.3	Product Data Standards	E-4
1.4	Text Description Standards	E-5
2.0	Standard Data Access Protocols	E-5
3.0	Application-Specific Data Models	E-6
4.0	Data Modeling Methods	E-6
5.0	CALS Standards Testing	E-7

SURVEY OF RELEVANT STANDARDS DEVELOPMENT EFFORTS

1.0 DATA FORMATS

A large number of standards can be used for communicating specific application data. Many protocols can be used to transmit the same data with different levels of semantic content. Multiple data formats will be required first for compatibility with a wide range of systems, and second to represent the various classes of semantic content associated with specific objects (for example, to avoid transmitting a full set of engineering information when the user needs only a hard copy of a drawing). We describe several classes of data formats and specific standards below.

1.1 Facsimile Transmission Standards

The Consultative Committee for International Telephony and Telegraphy (CCITT) has defined several facsimile transmission standards to provide for the transfer of raster-scanned images of text or graphics such as line drawings. These standards generally do not provide for transmission of attributes associated with color and gray scale. In general they can be used only to transmit images for printing or display using a resolution and color or gray scale close to those at which the image was originally scanned. They are appropriate primarily for transmission of data generated by scanning paper or microfilm.

1.2 Graphics Standards

The Computer Graphics Metafile (CGM) contains device-independent, digitally encoded vector graphics data. CGM files are easily transferred and displayed on a wide variety of hard-copy devices. They are usually more compact than either facsimile or the Initial Graphics Exchange Specification (IGES) files and would provide a potential standard for transmitting graphics data within Computer-aided Acquisition and Logistic Support (CALS).

The Programmer's Hierarchical Interactive Graphics Standard (PHIGS) is an emerging graphics programming standard to provide an application programmer's interface to a device-independent graphics environment. It is designed to remedy the lack of hierarchies in the International Standards Organization (ISO) Graphical

Kernel Standard (GKS), so that graphical objects can be used without representing each object explicitly. It is useful for computer-aided design (CAD), computer-aided engineering (CAE), computer-aided manufacturing (CAM), command and control, molecular modeling, simulation, and process control. PHIGS emphasizes the support of applications needing a highly dynamic, highly interactive operator interface and relies upon rapid screen update of the complex images being performed by the display system. Initial implementations will be designed to run on high-performance systems. In the future, it may run on workstations and be an appropriate standard for CALS data display.

1.3 Product Data Standards

IGES is the only product data exchange standard currently accepted as an international standard. It is a neutral format for translating data from one CAD system to another. However, because there are subtle semantic issues that can make it difficult to transfer exactly all the information in a drawing, it is sometimes not possible to translate into IGES. IGES is an obvious candidate as a format for data exchange within CALS, partly because of its support for text, which would allow it to support mixed text and graphical databases, except where the textual structure is too complex for IGES text facilities.

The Product Data Exchange Specification (PDES) is being developed to support advanced manufacturing and planning systems. PDES is viewed as a more advanced technology, rather than a replacement for IGES, to describe the complete set of information needed to manufacture a part. A workable PDES capability is still a few years away from quality vendor implementation; however, a working draft description is available.

The VHSIC[1] Hierarchical Definition Language (VHDL) and the Electronic Data Interchange Format (EDIF) are proposed standards for documentation of integrated circuit designs in particular, and electronic designs in general. They overlap with standards such as IGES and PDES in the area of printed circuit board design.

[1]Very High Speed Integrated Circuit.

1.4 Text Description Standards

The Standard Generalized Markup Language (SGML) uses an approach similar to that used in IBM's Generalized Markup Language (GML) and in the UNIX Nroff/Troff text formatters. It provides authors the benefits of a high-level markup language in which complex formatting procedures can be invoked by simple tags while simultaneously providing uniformity of style across documents and independence from any specific output device. It may be adaptable to mixed text and graphics data, in which the presence of graphics data in a standard format, such as CGM or IGES, is marked and processing capabilities are provided.

2.0 STANDARD DATA ACCESS PROTOCOLS

Structured Query Language (SQL) and Network Data Language (NDL) are standard languages for user and application program data access that are based, respectively, on the relational and network data modeling methods. The Remote Data Access Protocol (RDAP) is a standard communications protocol being developed for requesting execution of SQL at a remote site. SQL (and RDAP) will need to be supported by CALS gateways because of widespread use. However, SQL will probably not be sufficient as a data access language since it is not object-oriented and is semantically weak for expressing engineering data.

Requirements have also been developed for extensions to the Common Ada Interface Set (CAIS) for data access protocols. CAIS is currently being developed by DoD to provide an interface between Ada programs and operating system services. The data access extensions require at least the power of an entity-relationship model. They cannot be met by SQL.

Other standard protocols provided for ISO Layers 6 and 7 include Common Application Service Elements (CASE) and Specific Application Service Elements (SASE), as well as the Descriptive Data File (DDF) and Abstract Syntax Notation (ASN.1). Both ASN.1 and DDF are concerned with transferring application-defined data types in hierarchically nested data structures. DDF can be used for transparent interchange of physical recorded media as well as communications media, where the contents can be in any internationally recognized character set and coding. ASN.1 is an ISO Draft Standard language for defining hierarchically nested data structures, rather than a syntax for specifying columns and row occurrences (like DDF).

3.0 APPLICATION-SPECIFIC DATA MODELS

Much of the work on application-specific data models has been done in the context of data exchange standards. The Air Force's Product Data Definition Interface (PDDI) project and the related PDES standardization effort are developing a set of application-specific data models in order to define such standardized formats. However, no standardized data modeling method has been selected yet by these groups.

The Air Force's Integrated Design Support (IDS) contract is currently developing a data model using the Integrated Computer-Assisted Manufacturing (ICAM) method. This model describes the relationship of parts and documents throughout the weapon system's life cycle.

The VHSIC/Executive Information System (EIS)/Engineering Information Model (EIM) will be developed as a part of the VHSIC/EIS program. The EIM is intended to capture detailed semantics of engineering data associated with the development of integrated circuits. As such, it will provide a context for new engineering and will encompass the semantics associated with VHDL and EDIF languages.

Other standardization efforts in this area include work by the Institute of Electrical and Electronic Engineers (IEEE) Design Automation Standards Subcommittee (DASS) Working Group on Information Modeling (WGIM).

4.0 DATA MODELING METHODS

Data modeling methods are formalized means of capturing the semantics of data whose syntax is specified by data formats. They provide the means of specifying data structure and built-in operations for manipulating data specified by the method. Relevant methods include the classical models of database management systems (i.e., relational, network, and hierarchical), entity-relationship models, various "semantic" models, and other specialized methods for capturing the semantics of engineering disciplines. SQL is, in fact, a data access protocol based on the relational modeling method.

ICAM Definition (IDEF)1X, a method developed by the Air Force as a part of the ICAM program, is based on the entity-relationship model. Though it can capture some of the semantics of entity interrelationships, it cannot formally capture the

semantics of specific relationships, nor of specific data fields or values. (These kinds of semantics are captured in IDEF1X using comments and other human-readable documentation techniques.)

The PROBE data model is an object-oriented method and a formalized algebra for manipulating data developed under sponsorship of the Space and Naval Warfare Systems Command (SPAWAR). Data models built using this method can describe a wide range of application-specific semantics.

5.0 CALS STANDARDS TESTING

The CALS project has initiated standards testing through a joint DoD-industry CALS Test Network (CTN). This network, which will eventually include Government, defense contractor, and university sites, will emphasize the development of product conformance test and test procedures. Such testing will verify the implementation of CALS standards and the interoperation of various vendor products. This network will provide for end-to-end product transmission with linkage through telecommunications or through transmitted physical media.

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT "A" Approved for public release; distribution unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) LMI-PL810R1	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Logistics Management Institute 6b. OFFICE SYMBOL *(If applicable)*	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS *(City, State, and ZIP Code)* 6400 Goldsboro Road Bethesda, Maryland 20817-5886	7b. ADDRESS *(City, State, and ZIP Code)*
8a. NAME OF FUNDING / SPONSORING ORGANIZATION OASD(P&L) 8b. OFFICE SYMBOL *(if applicable)* ODASD (Systems)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER MDA903-85-C-0139
8c. ADDRESS *(City, State, and ZIP Code)* The Pentagon, Room 3E808 Washington, DC 20301	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
Computer-Aided Acquisition and Logistic Support Telecommunications Plan

12. PERSONAL AUTHOR(S)
John S. Doby

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(Year, Month, Day)*	15. PAGE COUNT
Final	FROM _____ TO _____	August 1989	177

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUB-GROUP	CALS, gateways, GOSIP, DDN

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

This report recommends a telecommunications architecture that specifies communications protocols, data exchange protocols, and transmission media to support CALS projects. The plan recommends implementation in three phases, consistent with the phased Department of Defense migration to Open Systems Interconnection (OSI) standards.

This report also recommends an intelligent gateway (IG) architecture to facilitate retrieval and analysis of data, by logisticians, from distributed applications using dissimilar hardware and software. This access will not require changes to existing databases, database management systems, or application programs.

This plan is designed to assist in the development of organization-specific communications plans tailored to each CALS effort.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS		
22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE *(Include Area Code)*	22c. OFFICE SYMBOL